Symmetries of matrix multiplication algorithms. I.

Vladimir P. Burichenko

Institute of mathematics of National Academy of Sciences of Belarus
Kirov Street 32a, Gomel 246000, Republic of Belarus
vpburich@gmail.com

Abstract

In this work the algorithms of fast multiplication of matrices are considered. To any algorithm there associated a certain group of automorphisms. These automorphism groups are found for some well-known algorithms, including algorithms of Hopcroft, Laderman, and Pan. The automorphism group is isomorphic to $S_3 \times Z_2$ and S_4 for Hopcroft anf Laderman algorithms, respectively. The studying of symmetry of algorithms may be a fruitful idea for finding fast algorithms, by an analogy with well-known optimization problems for codes, lattices, and graphs.

Keywords: Strassen algorithm, symmetry, fast matrix multiplication.

1 Introduction

In the present work we study algorithms of fast multiplication of matrices. This work is a continuation of the previous work of the author [13] (but it can be read idependently of [13]. It is even preferable to read the present work before [13], because some basic concepts are exposed here better than in [13]).

In 1969 V.Strassen [42] found an algorithm for multiplication of two $N \times N$ matrices, requiring $O(N^\tau)$ (or, more exactly, $\leq 4.7N^\tau$) arithmetical operations; here $\tau = \log_2 7 = 2.808\ldots$. (Recall that the usual algorithm ("multiplying a row by a column") requires $2N^3 - N^2$ operations). This algorithm is based on the fact, discovered by Strassen, that two 2×2 matrices with non-commuting elements, i.e., matrices over an arbitrary associative ring R, can be multiplied using only 7 multiplications in R.

Later some algorithms, asymptotically faster than Strassen's, were found. We give a very short survey of the related works in the end of this section.

The subject of the present work is studying symmetry of algorithms. The author thinks that using symmetry may be a fruitful way to find good algorithms.

Very short and clear exposition of the Strassen algorithm (appropriate for a student) may be found in some textbooks on linear algebra or computer algorithms. See, for example, [32], §I.4, Ex.12, or [1], §6.2. An introduction to the whole area of fast matrix multiplication may be found in book [12] or survey [34]. The books [22], [9], and Section 4.6.4 of [29] also should be mentioned. Nevertheless, the author tried to make the present work self-contained, so in this Introduction and the next section all necessary concepts, related to matrix multiplication algorithms, are recalled. Also, in Subsection 1.3 are contained some directions concerning literature in algebra.

1.1 Definition of an algorithm

An algorithm for the multiplication of matrices of given size may be described either in computational (i.e., as a sequence of computations), matrix, or tensor form.

To give an example of an algorithm in computational form, we recall the description of the Strassen algorithm. Let R be arbitrary (associative) ring, and let

$$X = \begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix}, \qquad Y = \begin{pmatrix} y_{11} & y_{12} \\ y_{21} & y_{22} \end{pmatrix}$$

be matrices over R. Consider the following products:

$$p_1 = x_{11}(y_{12} + y_{22}), \quad p_2 = (x_{11} - x_{12})y_{22}, \quad p_3 = (-x_{21} + x_{22})y_{11},$$

$$p_4 = x_{22}(y_{11} + y_{21}), \quad p_5 = (x_{11} + x_{22})(y_{11} + y_{22}),$$

$$p_6 = (x_{11} + x_{21})(y_{11} - y_{12}), \quad p_7 = (x_{12} + x_{22})(y_{21} - y_{22}).$$

Next, take linear combinations

$$z_{11} = -p_2 - p_4 + p_5 + p_7, \quad z_{12} = p_1 - p_2,$$

$$z_{21} = -p_3 + p_4, \quad z_{22} = -p_1 - p_3 + p_5 - p_6.$$

It is easy to check that these z_{ij} are nothing else but the elements of the matrix $Z = XY$. Thus, we have computed the product of X and Y, using only 7 multiplications (but 18 additions/subtractions) in R.

Further, describe what is the matrix form of an algorithm. Let m, n, p, and r be natural numbers, K be a field. Take symbols x_{ij} and y_{jk}, where $1 \le i \le m$, $1 \le j \le n$, $1 \le k \le p$ ($mn + np$ symbols total), and let

$$A = K\langle x_{ij}, y_{jk} \mid i, j, k \rangle$$

be the free associative algebra over K generated by these symbols. Next, suppose we are given field elements a_{ijl}, b_{jkl}, $c_{ikl} \in K$, for $1 \le i \le m$, $1 \le j \le n$, $1 \le k \le p$, $1 \le l \le r$; we may think of them as elements of $3r$ matrices

$$a_l = (a_{ijl})_{1\le i\le m,\ 1\le j\le n}, \qquad b_l = (b_{jkl})_{1\le j\le n,\ 1\le k\le p},$$

$$c_l = (c_{ikl})_{1\le i\le m,\ 1\le k\le p}, \qquad l = 1, \dots, r.$$

Suppose that the following mp relations in A are true:

$$\sum_{l=1}^{r} c_{ikl}\Big(\sum_{\substack{1\le u\le m\\ 1\le v\le n}} a_{uvl}x_{uv}\Big)\Big(\sum_{\substack{1\le v\le n\\ 1\le w\le p}} b_{vwl}y_{vw}\Big) = \sum_{j=1}^{n} x_{ij}y_{jk}\,, \tag{1}$$

for all $1 \le i \le m$, $1 \le k \le p$. Then we say that the set of r triples of matrices

$$\mathcal{A} = \{(a_l, b_l, c_l) \mid l = 1, \dots, r\}$$

is a *bilinear* (or *noncommutative*) algorithm over K for multiplication of an $m \times n$ matrix by an $n \times p$ matrix, *requiring* r *multiplications* (also called an algorithm *of length* r or *of bilinear complexity* r).

Indeed, let R be an arbitrary (associative) algebra over K, and let $Q = (q_{ij})$ and $S = (s_{jk})$ be $m \times n$ and $n \times p$ matrices, respectively, over R. Then one can compute their product $T = QS$ in the following way. First compute all linear combinations

$$d_l = \sum_{\substack{1 \le u \le m \\ 1 \le v \le n}} a_{uvl} q_{uv}, \qquad f_l = \sum_{\substack{1 \le v \le n \\ 1 \le w \le p}} b_{vwl} s_{vw} \,,$$

for all $1 \le l \le r$; then compute all products $p_l = d_l f_l$, and finally compute all linear combinations

$$t'_{ik} = \sum_{l=1}^{r} c_{ikl} p_l \,,$$

for all $1 \le i \le m$, $1 \le k \le p$. Then it follows from the relations (1) that $t'_{ik} = t_{ik}$ are precisely the elements of T. Thus, we have computed T, using r “nontrivial” (also called *non-scalar*) multiplications in R (here a *scalar* multiplication means a multiplication by an element of K). (It is well known that for algorithms of matrix multiplication the number of multiplications is most important. In particular, if there exists a non-commutative algorithm $\mathcal{A}$ for multiplication of an $m \times n$ matrix by an $n \times p$ matrix, requiring r multiplications, then there is an algorithm for multiplication of two $N \times N$ matrices of complexity $O(N^\tau)$, where $\tau = 3 \log_{mnp} r$. On the other hand, the number of additions/subtractions and scalar (i.e., by an elements of K) multiplications in $\mathcal{A}$ affects only the constant factor in $O(N^\tau)$. The details may be found in the literature).

Example. It is easy to see that the Strassen algorithm may be written in matrix form as the following set of seven triples of matrices:

$$\left(\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & -1 \end{pmatrix} \right), \quad \left(\begin{pmatrix} 1 & -1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & -1 \\ 0 & 0 \end{pmatrix} \right),$$

$$\left(\begin{pmatrix} 0 & 0 \\ -1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ -1 & -1 \end{pmatrix} \right), \quad \left(\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 1 & 0 \end{pmatrix} \right),$$

$$\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right), \quad \left(\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & -1 \end{pmatrix} \right),$$

$$\left(\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \right).$$

We will denote the Strassen algorithm by $\mathcal{S}$.

A description of what is an algorithm in tensor form will be given in Section 2.

1.2 Motivation, the aim of the work, and the results

By $r_K(m, n, p)$ we denote the minimal number of multiplications in a bilinear algorithm over a field K for multiplication of an $m \times n$ matrix by an $n \times p$ matrix. In principle, $r_K(m, n, p)$ may depend on K, but the author does not know any particular example of m, n, p, K_1

and K_2 such that $r_{K_1}(m,n,p) \neq r_{K_2}(m,n,p)$ (but, in the author's opinion, such examples certainly must exist).

It is widely recognized that finding of $r_K(m,n,p)$ for small m, n, p is an important problem, both from theoretical and practical viewpoint. The greatest interest at the moment is attracted by $r(3,3,3)$.

For small m, n, p the following estimates are known (for any K).

- $r(2,2,2) = 7$. The inequality $r(2,2,2) \leq 7$ follows from the existence of the Strassen algorithm. The opposite inequality $r(2,2,2) \geq 7$ was first proved in [46], and later several other proofs were found.
- $r(2,2,3) = 11$, $r(2,2,4) = 14$, $17 \leq r(2,2,5) \leq 18$. Here the upper estimates easily follow from the Strassen algorithm, and the lower ones were proved by V.B.Alekseev in works [2], [3], [4], respectively.
- $14 \leq r(2,3,3) \leq 15$, $19 \leq r(3,3,3) \leq 23$. Here the upper estimates follow from the algorithms contained in the works [23] and [33] respectively (we recall these algorithms in Sections 6 and 5). The lower estimates were proved by Bläser in works [7] and [8], respectively.

It is also well known that $r(m,n,p)$ is symmetric in m, n, and p, and that $r(m,n,1) = mn$.

It should be noted that in the case when $K = GF(2) = \{0,1\}$, or if the coefficients of algorithms are supposed to be integers, there are some further results (see [23] and [24]).

It may be a good idea in the search for economical algorithms that such algorithms may have many symmetries, that is, a large automorphism group. (It will be explained later in the article what we mean by an automorphism of an algorithm). Note that one faces the similar situation when studying codes, lattices, or graphs. Good (that is, dense) lattices and codes often have large group of automorphisms (see [15] for numerous examples of this phenomenon). Similarly, the graphs satisfying certain regularity conditions (distance regular graphs, especially those with "extremal" set of parameters) often have large automorphism group; see [11].

In [13] the author has proved that the Strassen algorithm $\mathcal{S}$ has the automorphism group $\mathrm{Aut}(\mathcal{S}) \cong S_3 \times S_3$, or even $S_3 \times D_6$, if we consider automorphisms in some "extended" sense. Here S_3 is the symmetric group on 3 letters, and D_6 is the dihedral group of order 12 (i.e., the group of all symmetries of a regular hexagon).

It should be noted that $\mathcal{S}$ is, in a sense, unique: any other algorithm for multiplication of two 2×2 matrices requiring 7 multiplications is conjugate to $\mathcal{S}$ under certain transformation group. See [20], [21].

Before trying to find good algorithms with large automorphism groups in unknown cases (say, for multiplication of 3×3 matrices), it is a reasonable first step to study automorphisms of some good algorithms known so far. This is the aim of the present work.

J.E.Hopcroft found an algorithm for multiplying of 3×2 matrix by a 2×3 matrix, requiring 15 multiplications. This algorithm is described in [23], and more accurately in [24]. We denote the Hopcroft algorithm by $\mathcal{H}$.

J.Laderman [33] found an algorithm for multiplication of two 3×3 matrices requiring 23 multiplications. We denote this algorithm by $\mathcal{L}$.

V.Ya.Pan (see, for example, [39]) described several algorithms for multiplication of matrices of arbitrary size, known as the *trilinear aggregation algorithms*. The most known of them is an algorithm for multiplication of two $n \times n$ matrices, where $n = 2m$ is even, requiring $(n^3 - 4n)/3 + 6n^2$ multiplications. We denote this algorithm by $\mathcal{P}_{2m}$.

One of the main results of the present work is the following theorem.

Theorem 1.1 *Let $\mathcal{H}$, $\mathcal{L}$, and $\mathcal{P}_{2m}$ be the algorithms of Hopcroft, Laderman and Pan, mentioned above. Then*

$$\mathrm{Aut}(\mathcal{H}) \cong S_3 \times Z_2 \,,$$

$$\mathrm{Aut}(\mathcal{L}) \cong S_4 \,,$$

and

$$\mathrm{Aut}(\mathcal{P}_{2m}) \cong S_m \times Z_2 \times S_3 \,.$$

(Of course, we will give a description of automorphism groups, mentioned in this theorem, not only up to isomorphism, but in an explicit form).

1.3 Some further remarks

Remark 1. Since Strassen's work, other estimates for asymptotic complexity of matrix multiplication (better than $O(N^{2.81})$) were found. The authors who contributed to these investigations are (approximately in chronological order) Pan, Bini/Capovani/Lotti/Romani, Schönhage, Strassen, and Coppersmith/Winograd. The most significant progress was made due to the so-called "laser method" of Strassen. The details and references may be found in the literature, see for example Chapter 15 of [12] and the introduction to [45]. The most recent works belong to Stothers [41], Vassilevska-Williams [44] (see also [45]), and Zhdanovich [49]. In [44] and [49], independently, the estimation $O(N^\omega)$ with $\omega < 2.373$ was proved.

It should be said that in all these estimations the constant factor in $O(N^\omega)$ is very large, so that the corresponding algorithms are only of theoretical interest and are useless in practice. For practical purposes only the following algorithms may be used: the usual algorithm, the Strassen algorithm, the Pan trilinear aggregation method, and the "compound" algorithms (which will be mentioned in the next remark).

Remark 2. There are other types of algorithms for matrix multiplication, different from bilinear algorithms as described above. Namely, there are

- *commutative* (or *quadratic*) algorithms, which may be used if we suppose that elements of matrices belong to a commutative ring; see [47] or [36] for the examples of such algorithms, and §14.1 of [12] for general definition;
- *approximate* algorithms, like in [6] (see [12], §15.2 for further explanations);
- *"compound"* bilinear algorithms, that is, the algorithms assembled, in an appropriate way, from several algorithms of smaller formats. The work [18] contains a survey of such algorithms.

The algorithms of all these three types are *not* considered in the present work.

Remark 3. The present text is written in a manner a bit different from the usual journal article. The author means that he gives more details than it is usual in a journal. So the reader may find some places trivial. The reason is that the author wishes that the text could be readable both by specialists in algebra and by computer scientists; but these specialists may have modest background in computer science or algebra, respectively.

The author would like to give some references / reading suggestions for readers who may be not very experienced in algebra (say, computer scientists).

The reader can use textbooks [31], [5], and [32] as a basic course in general and linear algebra (including the basics of the group representation theory). The book [48] contains a very lucid exposition of multilinear algebra (i.e., the theory of tensors). The last chapter of [32] is also devoted to multilinear algebra. The book [16] is a classical (but not elementary) source for group representation theory); chapters 1 and 2 are especially recommended to the reader. There is also an elementary and application-oriented textbook [26]. Finally, we should list some graduate-level algebra courses, namely [35], [25], and [19].

Structure of the work. The work is organized as follows. In Section 2 we recall the relations between matrix multiplication algorithms and decompositions of tensors. Section 3 contains general considerations on symmetry of tensors and algorithms. In a long Section 4 we find the isotropy group of the structure tensor of matrix multiplication map (which is a necessary preliminary step for studying automorphisms of any particular algorithm). In Sections 5 and 6 we find automorphism groups of Laderman and Hopcroft algorithms, respectively.

In Part II of the work Pan's trilinear aggregation algorithm, and some other topics, will be considered.

Acknowledgement. The author thanks A.S.Kleshchev for useful literature directions.

2 Tensor form of an algorithm

Let $V_1, \ldots, V_l$ be vector spaces over a field K, $\widetilde{V} = V_1 \otimes \ldots \otimes V_l$ be their tensor product. A tensor $t \in \widetilde{V}$ is *decomposable* if $t = v_1 \otimes \ldots \otimes v_l$, for some $v_i \in V_i$, $i = 1, \ldots, l$. We will consider representations of a tensor $t \in \widetilde{V}$ in the form $t = t_1 + \ldots + t_s$, where $t_1, \ldots, t_s$ are decomposable tensors. The least possible length s of such a representation is called the *rank* of t, and is denoted by $\mathrm{rk}(t)$. Obviously, $\mathrm{rk}(t) = 1$ if and only if t is decomposable.

In the situation described the following terminology is also used: the set $\{t_1, \ldots, t_s\}$ is called an *algorithm* (of length s), *computing* t.

By $M_{mn}(K)$ (or just M_{mn}) we denote the space of all $m \times n$ matrices over K. The basis of $M_{mn}(K)$ is $(e_{ij} \mid 1 \le i \le m,\ 1 \le j \le n)$, where e_{ij} are usual matrix units.

In the sequel an important role is played by the tensor

$$\langle m, n, p \rangle = \sum_{1 \le i \le m,\ 1 \le j \le n,\ 1 \le k \le p} e_{ij} \otimes e_{jk} \otimes e_{ki} \ \in M_{mn} \otimes M_{np} \otimes M_{pm} \,.$$

(Here two remarks concerning notation are in order: (1) Note that we have abused notation a bit, by using the similar symbols e_{ij} and e_{jk} for elements of different spaces; (2) in [13] the tensor $\langle m, n, p \rangle$ was denoted by $S(m, n, p)$. The notation $\langle m, n, p \rangle$, which is now classical, is due to Schönhage.)

It is a classical fact (first established by Strassen) that there is a bijection between the set of all algorithms for multiplication of an $m \times n$ matrix by an $n \times p$ matrix requiring r multiplications, and the set of all algorithms of length r computing $\langle m, n, p \rangle$. The following proposition gives an explicit description of this bijection. Note that in condition (a) of this proposition we think of matrices as tables whose elements are elements of K, so that

$$a = (a_{ij})_{1\le i\le m,\ 1\le j\le n}\ ,$$

whereas in condition (b) we think of matrices as elements of linear spaces, so that

$$a = \sum_{1\le i\le m,\ 1\le j\le n} a_{ij}e_{ij}\ .$$

As usually, by x^t and δ_{ab} we denote the transposed matrix and the Kronecker delta symbol.

Proposition 2.1 *Let $m, n, p, r \in \mathbb{N}$, and let K be a field. Let*

$$a_l = (a_{ijl})_{1\le i\le m,\ 1\le j\le n}\ , \quad b_l = (b_{jkl})_{1\le j\le n,\ 1\le k\le p}\ , \quad \textit{and } c_l = (c_{ikl})_{1\le i\le m,\ 1\le k\le p}\ ,$$

where $l = 1, \dots, r$, be matrices over K, of sizes $m\times n$, $n\times p$, and $m\times p$, respectively.

Then the following three conditions are equivalent:

(a) $\{(a_l, b_l, c_l) \mid l = 1, \dots, r\}$ is a bilinear algorithm over K for multiplication of an $m\times n$ matrix by an $n\times p$ matrix;

(b) $\{a_l \otimes b_l \otimes (c_l)^t \mid l = 1, \dots, r\}$ is an algorithm computing tensor $\langle m, n, p\rangle$;

(c) the following $(mnp)^2$ equations, for all $1 \le i, i_1 \le m$, $1 \le j, j_1 \le n$, and $1 \le k, k_1 \le p$, are satisfied:

$$\sum_{l=1}^{r} a_{ijl}b_{j_1kl}c_{i_1k_1l} = \delta_{ii_1}\delta_{jj_1}\delta_{kk_1}\ . \tag{2}$$

Proof. First we prove that conditions (a) and (c) are equivalent. Consider relation (1) of the Introduction,

$$\sum_{l=1}^{r} c_{ikl}\Big(\sum_{\substack{1\le u\le m\\ 1\le v\le n}} a_{uvl}x_{uv}\Big)\Big(\sum_{\substack{1\le v\le n\\ 1\le w\le p}} b_{vwl}y_{vw}\Big) = \sum_{j=1}^{n} x_{ij}y_{jk},$$

for a given pair (i, k). Clearly, this relation is true if and only if the coefficients at $x_{ef}y_{gh}$ on both sides coincide, for every quadruple (e, f, g, h) such that $1 \le e \le m$, $1 \le f, g \le n$, $1 \le h \le p$. It is easy to see that the coefficient on the left is $\sum_{l=1}^{r} c_{ikl}a_{efl}b_{ghl}$, and the coefficient on the right is $\delta_{ie}\delta_{fg}\delta_{kh}$. Thus we obtain the condition

$$\sum_{l=1}^{r} c_{ikl}a_{efl}b_{ghl} = \delta_{ie}\delta_{fg}\delta_{kh}\ ,$$

for all i, k, e, f, g, h such that $1 \le i, e \le m$, $1 \le f, g \le n$, $1 \le h, k \le p$. But the latter condition coincides with the equality in condition (c), up to names of indices (namely, e, f, g, h, i, k should be changed to i, j, j_1, k, i_1, k_1, respectively).

In a similar way one can prove that conditions (b) and (c) are equivalent too. Indeed, condition (b) means that

$$\sum_{l=1}^{r} a_l \otimes b_l \otimes (c_l)^t = \langle m, n, p\rangle.$$

Now it is sufficient to observe that the tensors of the form $e_{ij}\otimes e_{j_1k}\otimes e_{k_1i_1}$, where $1 \le i, i_1 \le m$, $1 \le j, j_1 \le n$, and $1 \le k, k_1 \le p$, form the basis of $M_{mn} \otimes M_{np} \otimes M_{pm}$, and to calculate the coefficients at basis elements in both sides of the latter relation.

Finally, the conditions (a) and (b) are equivalent, because each of them is equivalent to (c). □

Let $\mathcal{A} = \{(a_l, b_l, c_l) \mid l = 1, \ldots, r\}$ be an algorithm for multiplication of an $m \times n$ matrix by an $n \times p$ matrix, and let $\mathcal{A}' = \{a_l \otimes b_l \otimes c_l^t \mid l = 1, \ldots, r\}$ be the corresponding algorithm computing $\langle m, n, p\rangle$. Then we say that $\mathcal{A}'$ is the *tensor form* of $\mathcal{A}$.

Example. In the Introduction we have recalled Strassen algorithm and have written it in matrix form. It is readily seen that in the tensor form this algorithm is

$$\begin{aligned}\mathcal{S} = \{ \quad & e_{11} \otimes (e_{12} + e_{22}) \otimes (e_{21} - e_{22}),\ (e_{11} - e_{12}) \otimes e_{22} \otimes (-e_{11} - e_{21}),\\ & (-e_{21} + e_{22}) \otimes e_{11} \otimes (-e_{12} - e_{22}),\ e_{22} \otimes (e_{11} + e_{21}) \otimes (-e_{11} + e_{12}),\\ & (e_{11} + e_{22}) \otimes (e_{11} + e_{22}) \otimes (e_{11} + e_{22}),\ (e_{11} + e_{21}) \otimes (e_{11} - e_{12}) \otimes (-e_{22}),\\ & (e_{12} + e_{22}) \otimes (e_{21} - e_{22}) \otimes e_{11}\ \}.\end{aligned}$$

Remark. The reader can check directly that the sum of the tensors of the latter set is $\langle 2, 2, 2\rangle$. Such a checking can be considered as an evidence that we had made no mistakes when finding the matrix form of the Strassen algorithm from its computational form, and then the tensor form from the matrix form.

The equations (2) first appeared in [10], so they are called *Brent equations* (but it is possible that similar equations appeared earlier in studying decompositions of general tensors, see [30]).

One of approaches to finding algorithms for matrix multiplication is to solve Brent equations, usually by computer calculations. To do this, one usually reduces solving the Brent equations to finding minima of certain real-valued function of many (several hundreds) variables, and then solves this optimization problem by numerical methods. See [10], [27] for more details. Other works in this direction are [37] and [40]. In works [14] and [33] the Brent equations are also used, but in a different way (without numerical optimization).

3 Group actions on tensors and algorithms

Let $U_1, \ldots, U_m$ and $V_1, \ldots, V_n$ be spaces over a field K, and let $\widetilde{U} = U_1 \otimes \ldots \otimes U_m$ and $\widetilde{V} = V_1 \otimes \ldots \otimes V_n$ be their tensor products. By a *decomposable isomorphism* we mean an isomorphism of vector spaces $\varphi : \widetilde{U} \to \widetilde{V}$ such that there are a bijection $\tau : \{1, \ldots, m\} \to \{1, \ldots, n\}$ (whence $m = n$) and isomorphisms $\varphi_i : U_i \to V_{\tau(i)}$ (whence $\dim V_{\tau(i)} = \dim U_i$ for all $i = 1, \ldots, m$) such that

$$\varphi(u_1 \otimes \ldots \otimes u_m) = \varphi_{\tau^{-1}(1)}(u_{\tau^{-1}(1)}) \otimes \ldots \otimes \varphi_{\tau^{-1}(m)}(u_{\tau^{-1}(m)})$$

for all $u_i \in U_i$, $i = 1, \ldots, m$.

For example, the usual permutation of factors $\pi : X \otimes Y \longrightarrow Y \otimes X$, $x \otimes y \mapsto y \otimes x$, is a decomposable isomorphism.

It is clear that the composition of two decomposable isomorphisms is a decomposable isomorphism also, and the isomorphism inverse to a decomposable isomorphism is decomposable too. It follows that a decomposable isomorphism $\varphi : \widetilde{U} \longrightarrow \widetilde{V}$ maps the set of all decomposable tensors in $\widetilde{U}$ bijectively onto the set of all decomposable tensors in $\widetilde{V}$.

If φ is a decomposable isomorphism defined by data $(\tau; \varphi_1, \ldots, \varphi_m)$, as in the first paragraph of this subsection, then we say that τ is a permutation, corresponding to φ (and φ is an isomorphism, corresponding to τ). For φ_i the similar terminology is used.

It is often convenient to think of the permutation τ, corresponding to φ, as a (bijective) map from set of factors $\{U_1 \ldots, U_m\}$ of $\widetilde{U}$ to the similar set $\{V_1, \ldots, V_m\}$ of $\widetilde{V}$. In particular, if $\widetilde{U} = \widetilde{V}$, then we may think of τ as a permutation of the set $\{U_1 \ldots, U_m\}$.

It is clear that if φ and ψ are decomposable isomorphisms, and σ and τ are permutations corresponding to φ and ψ, respectively, then $\rho = \sigma\tau$ is a permutation corresponding to the isomorphism $\theta = \varphi\psi$. Moreover, σ^{-1} is a permutation corresponding to φ^{-1}. (Note that we multiply permutations "from right to left", for example, $(134)(2) \cdot (14)(23) = (1)(243)$).

In general, the permutation (as well as the isomorphisms φ_i), corresponding to a given decomposable isomorphism φ, is defined by φ not uniquely. Consider two examples.

Example 1. Let $m = 2$, $U_1 = \langle e_1 \rangle$, $U_2 = \langle e_2 \rangle$, $V_1 = \langle f_1 \rangle$, and $V_2 = \langle f_2 \rangle$ be one-dimensional spaces. Their tensor products $\widetilde{U} = U_1 \otimes U_2 = \langle e_1 \otimes e_2 \rangle$ and $\widetilde{V} = V_1 \otimes V_2 = \langle f_1 \otimes f_2 \rangle$ are one-dimensional also. Let $\varphi : \widetilde{U} \longrightarrow \widetilde{V}$ be the isomorphism taking $e_1 \otimes e_2$ to $f_1 \otimes f_2$. Then φ is the decomposable isomorphism corresponding to the permutation $\tau = e = \{1 \mapsto 1,\ 2 \mapsto 2\}$ and isomorphisms $\varphi_1 : e_1 \mapsto f_1$, $\varphi_2 : e_2 \mapsto f_2$. On the other hand, φ may be considered as the decomposable isomorphism, corresponding to permutation $\tau' = (1, 2) = \{1 \mapsto 2,\ 2 \mapsto 1\}$ and isomorphisms $\varphi'_1 : e_1 \mapsto f_2$, $\varphi'_2 : e_2 \mapsto f_1$.

Example 2. Let $\varphi_1 : U_1 \longrightarrow V_1$ and $\varphi_2 : U_2 \longrightarrow V_2$ be isomorphisms of spaces. Then the decomposable isomorphism

$$\varphi = \varphi_1 \otimes \varphi_2 \ : \ \widetilde{U} = U_1 \otimes U_2 \longrightarrow \widetilde{V} = V_1 \otimes V_2$$

can also be written as $\varphi = \varphi'_1 \otimes \varphi'_2$, where $\varphi'_1 = \lambda\varphi_1$ and $\varphi'_2 = \lambda^{-1}\varphi_2$, for any $\lambda \in K^*$.

It turns out that the possible ambiguity of data $(\tau; \varphi_1, \ldots, \varphi_m)$, corresponding to a given decomposable isomorphism φ, may be only of these two kinds. To prove this, we need two simple (and well-known) statements.

Lemma 3.1 *1) Suppose that $\varphi \in GL(V)$ is an automorphism of a space V such that $\varphi(\langle v \rangle) = \langle v \rangle$ for each one-dimensional subspace $\langle v \rangle \subseteq V$. Then φ is a multiplication by a scalar $\lambda \in K^*$.*

2) Let $\varphi, \varphi' : U \longrightarrow V$ be isomorphisms such that $\varphi(\langle u \rangle) = \varphi'(\langle u \rangle)$ for each one-dimensional subspace $\langle u \rangle \subseteq V$. Then there exists $\lambda \in K^*$ such that $\varphi' = \lambda\varphi$.

Proof. 1) Let $v_1, \ldots, v_n$ be a basis of V. As φ preserves all $\langle v_i \rangle$, we have $\varphi(v_i) = \lambda_i v_i$, for some elements $\lambda_i \in K^*$. Next, take any $i \neq j$. The vector $\varphi(v_i + v_j) = \lambda_i v_i + \lambda_j v_j$ must be proportional to $v_i + v_j$, whence $\lambda_i = \lambda_j$. Consequently, all $\lambda_1 = \lambda_2 = \ldots = \lambda_n$ coincide, whence φ is the multiplication by a scalar $\lambda = \lambda_1$.

2) It is obvious that $\theta = \varphi^{-1}\varphi'$ is an automorphism of U, and for any $u \in U$ we have $\theta(\langle u \rangle) = (\varphi^{-1}\varphi')(\langle u \rangle) = \varphi^{-1}(\varphi'(\langle u \rangle)) = \varphi^{-1}(\varphi(\langle u \rangle)) = \langle u \rangle$. Now we have $\theta = \lambda$ $(=\lambda \cdot \mathrm{id}_U)$ by 1), whence $\varphi' = \lambda\varphi$. □

Lemma 3.2 *Let $\widetilde{U} = U_1 \otimes \ldots \otimes U_m$ be the tensor product of several spaces, and for each $i = 1, \ldots, m$ let $T_i, T_i' \subseteq U_i$ be two nonzero subspaces. Then the subspaces*

$$\widetilde{T} = T_1 \otimes \ldots \otimes T_m \quad \text{and} \quad \widetilde{T}' = T_1' \otimes \ldots \otimes T_m' \subseteq \widetilde{U}$$

coincide if and only if $T_i = T_i'$ for all i. In particular, if $0 \neq t = u_1 \otimes \ldots \otimes u_m = u_1' \otimes \ldots \otimes u_m'$ are two decompositions of a nonzero decomposable tensor, then $\langle u_i \rangle = \langle u_i' \rangle$ for all $i = 1, \ldots, m$.

(The proof is left to the reader.)

Proposition 3.3 *Let $U_1 \ldots, U_m$ and $V_1, \ldots, V_m$ be two sets of m spaces each, and let $\widetilde{U} = U_1 \otimes \ldots \otimes U_m$ and $\widetilde{V} = V_1 \otimes \ldots \otimes V_m$ be their tensor products. Let $\tau, \tau' \in S_m$ be permutations such that $\dim V_{\tau(i)} = \dim V_{\tau'(i)} = \dim U_i$, let $\varphi_i : U_i \longrightarrow V_{\tau(i)}$ and $\varphi_i' : U_i \longrightarrow V_{\tau'(i)}$ be isomorphisms, and let $\varphi, \varphi' : \widetilde{U} \longrightarrow \widetilde{V}$ be the decomposable isomorphisms corresponding to the data $(\tau; \varphi_1, \ldots, \varphi_m)$ and $(\tau'; \varphi_1', \ldots, \varphi_m')$, respectively. Suppose that $\varphi = \varphi'$. Then the following two statements hold.*

1) $\tau' = \tau\sigma$, where σ is a permutation of $\{1, \ldots, m\}$ such that $\sigma(i) = i$ for all i such that $\dim U_i > 1$. *In particular, $\tau' = \tau$, if at most one of the spaces U_i is one-dimensional.*

2) Suppose that $\tau = \tau'$. Then there exist elements $\lambda_1, \ldots, \lambda_m \in K^*$ such that $\varphi_i' = \lambda_i \varphi_i$. For these λ_i we have $\lambda_1 \ldots \lambda_m = 1$.

Proof. 1) Define $\sigma = \tau^{-1}\tau'$. Then $\tau' = \tau\sigma$. It follows from the previous discussion that σ is a permutation corresponding to the decomposable automorphism $\theta = \varphi^{-1}\varphi'$ of $\widetilde{U}$. But, clearly, $\theta = 1 = \mathrm{id}_{\widetilde{U}}$. So it is sufficient to prove the following: if the decomposable automorphism θ of $\widetilde{U}$, defined by the data $(\sigma; \psi_1, \ldots, \psi_m)$ (where $\psi_i : U_i \longrightarrow U_{\sigma(i)}$ are some isomorphisms) coincides with $\mathrm{id}_{\widetilde{U}}$, then $\sigma(i) = i$ for all i such that $\dim U_i > 1$.

We may assume without loss of generality that $i = 1$. For each $j = 2, \ldots, m$ take a one-dimensional subspace $l_j \subseteq U_j$ and consider the subspace

$$W = U_1 \otimes l_2 \otimes \ldots \otimes l_m \subseteq \widetilde{U}.$$

Then $\theta(W) = X_1 \otimes \ldots \otimes X_m$, where $X_{\sigma(1)} = \psi_1(U_1) = U_{\sigma(1)}$, and $X_r = \psi_{\sigma^{-1}(r)}(l_{\sigma^{-1}(r)})$ for $r \neq \sigma(1)$. In particular, $\dim X_{\sigma(1)} > 1$ and $\dim X_j = 1$ if $j \neq \sigma(1)$.

Since $\theta(W) = W$, it follows from Lemma 3.2 that $X_1 = U_1$ and $X_j = l_j$ for $j \geq 2$. In particular, $\dim X_1 > 1$ and $\dim X_j = 1$ for $j \geq 2$. Consequently, $\sigma(1) = 1$.

2) Consider $\theta = \varphi^{-1}\varphi' = \mathrm{id}_{\widetilde{U}}$ again. It is rather clear that θ is the decomposable automorphism of $\widetilde{U}$, corresponding to $(e; \psi_1, \ldots, \psi_m)$, where e is the identity permutation of $\{1, \ldots, m\}$ and $\psi_i = \varphi_i^{-1}\varphi_i'$. That is, $\theta = \psi_1 \otimes \ldots \otimes \psi_m$. So it suffices to show that if $\psi_i \in GL(U_i)$ are some automorphisms such that $\theta = \psi_1 \otimes \ldots \otimes \psi_m = \mathrm{id}_{\widetilde{U}}$, then there exist $\lambda_1, \ldots, \lambda_m \in K^*$ such that $\psi_i = \lambda_i \mathrm{id}_{U_i}$, and that these λ_i satisfy the relation $\lambda_1 \ldots \lambda_m = 1$.

Take arbitrary nonzero elements $u_i \in U_i$, $u_i \neq 0$. Then $w = u_1 \otimes \ldots \otimes u_m \neq 0$, and $w = \theta(w) = \psi_1(u_1) \otimes \ldots \otimes \psi_m(u_m)$. It follows from Lemma 3.2 that $\langle \psi_i(u_i) \rangle = \langle u_i \rangle$ for all u_i. Since u_i were taken arbitrarily, it follows that $\psi_i(x)$ is proportional to x for all $x \in U_i$. By Lemma 3.1, there exists $\lambda_i \in K^*$ such that $\psi_i = \lambda_i \mathrm{id}_{U_i}$. Finally, $w = \psi_1(u_1) \otimes \ldots \otimes \psi_m(u_m) = \lambda_1 u_1 \otimes \ldots \otimes \lambda_m u_m = \lambda_1 \ldots \lambda_m w$, whence $\lambda_1 \ldots \lambda_m = 1$. □

In particular, we see that if at most one of the spaces U_i is one-dimensional, then for any decomposable automorphism φ of the space $\widetilde{U} = U_1 \otimes \ldots \otimes U_m$ the corresponding permutation of $\{U_1, \ldots, U_m\}$ is determined uniquely.

By $S(U_1, \ldots, U_m)$ we denote the group of all decomposable automorphisms of $\widetilde{U} = U_1 \otimes \ldots \otimes U_m$. Next, by $S^0(U_1, \ldots, U_m)$ we denote the subgroup of $S(U_1, \ldots, U_m)$ consisting of all automorphisms that preserve each factor U_i (that is, corresponding to the trivial permutation of $\{U_1, \ldots, U_m\}$). In other words, $S^0(U_1, \ldots, U_m)$ is the image of the homomorphism $GL(U_1) \times \ldots \times GL(U_m) \to GL(\widetilde{U})$ defined by

$$(g_1, \ldots, g_m) \mapsto g_1 \otimes \ldots \otimes g_m\,.$$

Clearly, $S^0(U_1, \ldots, U_m)$ is normal in $S(U_1, \ldots, U_m)$. The corresponding quotient group $T = S(U_1, \ldots, U_m)/S^0(U_1, \ldots, U_m)$ may be described as follows. Let $\Omega = \{U_i \mid \dim U_i > 1\}$ be the set of all factors U_i of dimension > 1, and let

$$T' = \{g \in \mathrm{Sym}(\Omega) \mid \dim g(X) = \dim X \quad \forall\; X \in \Omega\}$$

be the group of all permutations of these factors, preserving dimensions. Then it is easy to deduce from Proposition 3.3 that T can be identified with T' (the details are left to the reader).

Let $t \in \widetilde{U}$ be an arbitrary tensor. We call the set of all decomposable automorphisms of $\widetilde{U}$ that preserve t the *(full) isotropy group* of t, and denote it by $\Gamma(t)$:

$$\Gamma(t) = \{g \in S(U_1, \ldots, U_m) \mid g(t) = t\}.$$

We also consider the *small* isotropy group

$$\Gamma^0(t) = \Gamma(t) \cap S^0(U_1, \ldots, U_m).$$

Clearly, $\Gamma^0(t) \trianglelefteq \Gamma(t)$ and $\Gamma(t)/\Gamma^0(t)$ may be identified with a subgroup of the above-mentioned T (that is, with a certain group of permutations of factors of dimension > 1, preserving dimensions).

Finally, let $\mathcal{A} = \{t_1, \ldots, t_r\}$ be an algorithm computing t. Then

$$\mathrm{Aut}(\mathcal{A}) = \{g \in S(U_1, \ldots, U_m) \mid g(\mathcal{A}) = \mathcal{A}\}$$

will be called the *automorphism group* of $\mathcal{A}$. Obviously, $\mathrm{Aut}(\mathcal{A})$ preserves $t_1 + \ldots + t_r = t$, whence

$$\mathrm{Aut}(\mathcal{A}) \leq \Gamma(t).$$

If $u \in \widetilde{U}$, $v \in \widetilde{V}$, and $\varphi : \widetilde{U} \to \widetilde{V}$ is a decomposable isomorphism such that $\varphi(u) = v$, then $\mathrm{rk}(u) = \mathrm{rk}(v)$. Moreover, if $\mathcal{A}$ is an algorithm of length l, computing u, then $\mathcal{B} = \varphi(\mathcal{A})$ is an algorithm of length l, computing v (and conversely, if $\mathcal{B}$ is an algorithm of length l for v, then $\mathcal{A} = \varphi^{-1}(\mathcal{B})$ is an algorithm of length l for $\mathcal{A}$). Therefore, φ bijectively maps the set of all optimal algorithms computing u to the set of all optimal algorithms computing v.

In particular, we see that $\Gamma(t)$ acts on the set of all optimal algorithms computing t. Obviously, the stabilizer of a point (i.e., of an algorithm) with respect to this action is the automorphism group of a given algorithm.

Example. Let $U_1 = U_2 = U_3 = M_{22}(K)$ and $t = \langle 2,2,2\rangle \in U_1 \otimes U_2 \otimes U_3$. In this case it was shown by de Groote [21] that $\Gamma(t)$, and even $\Gamma^0(t)$, acts on the set of all optimal algorithms transitively, so this set is an orbit. The stabilizer (in the full $\Gamma(t)$) of a point in this orbit is nothing else but $\mathrm{Aut}(\mathcal{S})$, the automorphism group of the Strassen algorithm, which is isomorphic to $S_3 \times S_3$ by [13].

Remark. It is natural to consider more general situation, when studying decompositions of tensors, as it is done in [20]. Let $\mathcal{R}(\widetilde{U})$ be the set of all decomposable tensors in $\widetilde{U} = U_1 \otimes \ldots \otimes U_m$. A linear map $\varphi : \widetilde{U} \to \widetilde{V}$ is called a *Segre homomorphism*, if $\varphi(\mathcal{R}(\widetilde{U})) \subseteq \mathcal{R}(\widetilde{V})$. Next, let $t \in \widetilde{U}$, let $\varphi : \widetilde{U} \to \widetilde{U}$ be a Segre endomorphism such that $\varphi(t) = t$, and let $\mathcal{A}$ be an optimal algorithm computing t. Then $\varphi(\mathcal{A})$ is also an optimal algorithm computing t. So the semigroup of all Segre endomorphisms, preserving t, acts on the set of all optimal algorithms computing t. Thus one may think that studying of general Segre endomorphisms may be useful in algorithm analysis. However, it was, in fact, shown in [20] that such studying completely reduces to consideration of decomposable automorphisms.

4 The isotropy group of $\langle m, n, p\rangle$

Let $\mathcal{A} = \{t_1, \ldots, t_r\}$ be an algorithm computing the tensor $t = \langle m, n, p\rangle$. It was observed above that its automorphism group $\mathrm{Aut}(\mathcal{A})$ is contained in the (full) isotropy group $\Gamma(t)$:

$$\mathrm{Aut}(\mathcal{A}) \leq \Gamma(t).$$

So, before studying group $\mathrm{Aut}(\mathcal{A})$ for any particular algorithm $\mathcal{A}$, it is natural to find the group $\Gamma(t)$. This is the aim of the present section.

In the case $m = n = p$ the group $\Gamma(t)$ was already found, independently by Brockett-Dobkin, Strassen, and de Groote. Actually, Strassen and de Groote found $\Gamma(t)$ in the case where t is the structure tensor of a finite-dimensional simple K-algebra, that is, a matrix algebra over a skew field. See the comments after Theorem 3.3 of [20].

4.1 Some known facts

We begin with several standard statements.

Let $V = K^l$ be the space of columns of height l ($l \in \mathbb{N}$) with elements in K, let V' be the space of rows of the same length l, and $(e_1, \ldots, e_l)$ and $(e^1, \ldots, e^l)$ be the usual bases of V and V' (i.e., e_i is the column whose i-th element is 1, the others are equal to 0). Note that the rule $(v, v') \mapsto v'v$, where $v \in V$ and $v' \in V'$, defines nondegenerate bilinear map $V \times V' \longrightarrow K$ (pairing), and the bases (e_i) and (e^i) are dual with respect to this pairing (note that $v'v$ is an 1×1 matrix, i.e., an element of K). Thus, we may identify V' with V^*, the dual space of V.

Denote $G = GL_l(K)$. Then G acts on V on the left as usually: $(g, v) \mapsto gv$, where gv is the usual product of a matrix and a column. Also, there is a left action of G on V' by the rule

$$(g, v') \mapsto g \circ v' := v'g^{-1}.$$

(This is a left action indeed, that is, $(gh) \circ v' = g \circ (h \circ v')$ for all $g, h \in G$ and $v' \in V'$. Indeed, $g \circ (h \circ v') = g \circ (v'h^{-1}) = (v'h^{-1})g^{-1} = v'h^{-1}g^{-1} = v'(gh)^{-1} = (gh) \circ v'$.) So there is a left action of G on $V \otimes V' = V \otimes V^*$ such that

$$g(v \otimes v') = gv \otimes v'g^{-1} \qquad \forall g \in G,\ v \in V, v' \in V'.$$

Consider the tensor

$$\delta = \sum_{i=1}^{l} e_i \otimes e^i = \sum_{1 \le i,j \le n} \delta_{ij} e_i \otimes e^j \in V \otimes V^*$$

(so-called identity tensor, i.e., the tensor, associated with the identity linear map of V. Observe that the coefficients of the tensor δ are precisely δ_{ij}, where δ_{ij} is the Kronecker symbol. This justifies using the same symbol δ both for identity tensor and the Kronecker symbol).

The following lemma is well-known (even trivial; cf. Remark 3 in Subsection 1.3).

Lemma 4.1 *We have $g\delta = \delta$, for all $g \in G$.*

Proof. Let a_{ij} and b_{ij} be the coefficients of the matrices g and g^{-1}, i.e.,

$$g = \sum_{1 \le i,j \le l} a_{ij} e_{ij} \quad \text{and} \quad g^{-1} = \sum_{1 \le i,j \le l} b_{ij} e_{ij}.$$

Then $ge_i = \sum_{j=1}^{l} a_{ji} e_j$ and $e^i g^{-1} = \sum_{j=1}^{l} b_{ij} e^j$. Hence

$$\begin{aligned} g\delta &= g(\sum_{i=1}^{l} e_i \otimes e^i) = \sum_{i=1}^{l} ge_i \otimes e^i g^{-1} = \sum_{i=1}^{l} (\sum_{j=1}^{l} a_{ji} e_j) \otimes (\sum_{k=1}^{l} b_{ik} e^k) \\ &= \sum_{1 \le j,k \le l} (\sum_{i=1}^{l} a_{ji} b_{ik}) e_j \otimes e^k = \sum_{1 \le j,k \le l} (\delta_{jk}) e_j \otimes e^k = \sum_{j=1}^{l} e_j \otimes e^j = \delta, \end{aligned}$$

as $\sum_{i=1}^{l} a_{ji} b_{ik} = \delta_{jk}$ for all $1 \le j, k \le l$ (because matrices g and g^{-1} are inverse). □

Tensor products of group representations. Recall the notion of tensor product of representations of a group (see [31], §VIII.7, or [16], § 12). Let F be a field, G be a group, and let U and V be FG-modules, that is, F-spaces endowed with F-linear action of G. Let

$$T : G \longrightarrow GL(U) \quad \text{and} \quad R : G \longrightarrow GL(V)$$

be the corresponding representations of G on U and V. Put $W = U \otimes_F V$. For an element $g \in G$ define linear map $S(g) : W \longrightarrow W$ by $S(g) = T(g) \otimes R(g)$. Since both $T(g)$ and $R(g)$ are invertible, $S(g)$ is invertible also. Moreover,

$$\begin{aligned} S(g_1 g_2) &= T(g_1 g_2) \otimes R(g_1 g_2) = T(g_1)T(g_2) \otimes R(g_1)R(g_2) \\ &= (T(g_1) \otimes R(g_1))(T(g_2) \otimes R(g_2)) = S(g_1)S(g_2). \end{aligned}$$

That is,

$$S : g \mapsto S(g)\,, \qquad G \longrightarrow GL(W)$$

is a representation of G. It is called the *tensor product* of representations T and R (and W a tensor product of FG-modules U and V).

If U_1, U_2, V_1, and V_2 are FG-modules, and $\alpha : U_1 \longrightarrow U_2$ and $\beta : V_1 \longrightarrow V_2$ are FG-homomorphisms, then (as is easy to check) the map $\gamma = \alpha \otimes \beta : U_1 \otimes V_1 \longrightarrow U_2 \otimes V_2$ is a FG-homomorphism also.

4.2 A subgroup of $\Gamma^0(t)$

Let $D = K^m$, $E = K^n$, and $F = K^p$ be the spaces of columns over K of height m, n, and p, respectively, and D', E', and F' be the spaces of rows of the same length. By d_i, e_j, f_k, d^i, e^j, and f^k we denote the elements of the usual bases of $D, \ldots, F'$. As observed earlier, we may identify D', E' and F' with D^*, E^*, and F^*, respectively.

Note that for any $d \in D$ and $e' \in E'$ their product de' is an $m \times n$ matrix. In particular, $d_i e^j = e_{ij}$ are matrix units, for all $1 \le i \le m$, $1 \le j \le n$. Similarly for ef' and fd'.

Denote $M_{mn} = M_{mn}(K)$, M_{np} and M_{pm} by L_1, L_2, and L_3, respectively, and let

$$L = L_1 \otimes L_2 \otimes L_3 = M_{mn} \otimes M_{np} \otimes M_{pm}\,.$$

Also denote

$$N = D \otimes D' \otimes E \otimes E' \otimes F \otimes F'\,.$$

Next, define the linear map $\tau : N \to L$ by the rule

$$\tau : d \otimes d' \otimes e \otimes e' \otimes f \otimes f' \mapsto de' \otimes ef' \otimes fd'.$$

This map is well-defined indeed, because de', ef', and fd' are in L_1, L_2, and L_3, respectively, and, moreover, the expression $de' \otimes ef' \otimes fd'$ is linear in each of the arguments $d, d', \ldots, f'$.

It is easy to see that τ is an isomorphism of vector spaces.

Let $\delta_D = \sum_{i=1}^m d_i \otimes d^i$, δ_E and δ_F be the identity tensors of the spaces D, E, and F. Consider the tensors $\delta_D \otimes \delta_E \otimes \delta_F \in N$ and $\tau(\delta_D \otimes \delta_E \otimes \delta_F) \in L$.

Lemma 4.2 *The equality $\tau(\delta_D \otimes \delta_E \otimes \delta_F) = \langle m, n, p\rangle$ holds.*

Proof. We have

$$\begin{aligned}
\tau(\delta_D \otimes \delta_E \otimes \delta_F) &= \tau\left((\sum_{i=1}^m d_i \otimes d^i) \otimes (\sum_{j=1}^n e_j \otimes e^j) \otimes (\sum_{k=1}^p f_k \otimes f^k) \right) \\
&= \tau(\sum_{\substack{1\le i\le m\\ 1\le j\le n\\ 1\le k\le p}} d_i \otimes d^i \otimes e_j \otimes e^j \otimes f_k \otimes f^k) = \sum_{\substack{1\le i\le m\\ 1\le j\le n\\ 1\le k\le p}} d_i e^j \otimes e_j f^k \otimes f_k d^i \\
&= \sum_{1\le i\le m,\ 1\le j\le n,\ 1\le k\le p} e_{ij} \otimes e_{jk} \otimes e_{ki} = \langle m, n, p\rangle.
\end{aligned}$$

□

Next we consider some group actions. Put $G_D = GL_m(K)$, $G_E = GL_n(K)$, $G_F = GL_p(K)$. Then G_D acts on D and D', G_E — on E and E', and G_F acts on F and F'.

Form the direct product $G = G_D \times G_E \times G_F$ and define actions of G on $D, \ldots, F'$. For example, if $g = (g_1, g_2, g_3) \in G_D \times G_E \times G_F$, $d \in D$ and $d' \in D'$, then we define $g(d) = g_1 d$ and $g(d') = d' g_1^{-1}$ (here $g(d)$ and $g(d')$ mean the result of group action, and $g_1 d$ and $d' g_1^{-1}$ mean the products of matrices). That is, the factor G_D of G acts on D and D' as usually, whereas G_E and G_F act trivially. The actions on E, E', F, F' are defined similarly.

Now we can consider $N = D \otimes \ldots \otimes F'$ as a G-module.

Further, it is easy to see that the rules

$$(g_1, g_2, g_3)x = g_1 x g_2^{-1},\ g_2 x g_3^{-1}, \quad \text{or} \quad g_3 x g_1^{-1}$$

define actions of G on L_1, L_2, and L_3, respectively. Hence we can define action of G on $L = L_1 \otimes L_2 \otimes L_3$.

In the proof of the following lemma (and later) we use the following simple
Observation. Let K be a field, G a group, X and Y be KG-modules, and let $\varphi : X \longrightarrow Y$ be a K-linear map. If φ is a KG-module homomorphism and a K-spaces isomorphism, then φ is a KG-module isomorphism (that is, the inverse map $\varphi^{-1} : Y \longrightarrow X$ is a homomorphism of KG-modules).

Lemma 4.3 *The map $\tau : N \to L$, defined above, is a G-module isomorphism.*

Proof. As τ is an isomorphism of vector spaces, it remains to check that τ is a G-module homomorphism, that is, $\tau(g(x)) = g(\tau(x))$ for all $g \in G$ and $x \in N$.

It is sufficient to consider $x = d \otimes d' \otimes e \otimes e' \otimes f \otimes f'$. Let $g = (g_1, g_2, g_3)$. Then

$$\begin{aligned}
\tau(g(x)) &= \tau((g_1, g_2, g_3)(d \otimes d' \otimes e \otimes e' \otimes f \otimes f')) \\
&= \tau(g_1 d \otimes d' g_1^{-1} \otimes g_2 e \otimes e' g_2^{-1} \otimes g_3 f \otimes f' g_3^{-1}) \\
&= (g_1 d)(e' g_2^{-1}) \otimes (g_2 e)(f' g_3^{-1}) \otimes (g_3 f)(d' g_1^{-1}) \\
&= g_1 d e' g_2^{-1} \otimes g_2 e f' g_3^{-1} \otimes g_3 f d' g_1^{-1} = (g_1, g_2, g_3)(de' \otimes ef' \otimes fd') \\
&= g(\tau(x)).
\end{aligned}$$

(Note that there is an alternative way to prove that τ is a G-homomorphism. Namely, observe that the formula $x \otimes y \mapsto xy$ defines G-homomorphisms $\alpha : D \otimes E' \longrightarrow L_1$, $\beta : E \otimes F' \longrightarrow L_2$ and $\gamma : F \otimes D' \longrightarrow L_3$. So their product

$$\alpha \otimes \beta \otimes \gamma : D \otimes E' \otimes E \otimes F' \otimes F \otimes D' \longrightarrow L_1 \otimes L_2 \otimes L_3$$

is a G-homomorphism also. Also, the "permutation map"

$$\zeta : D \otimes D' \otimes E \otimes E' \otimes F \otimes F' \longrightarrow D \otimes E' \otimes E \otimes F' \otimes F \otimes D'$$

is obviously a G-homomorphism. Now it remains to observe that τ coincides with $(\alpha \otimes \beta \otimes \gamma) \circ \zeta$. □

The proof of the following simple lemma is left to the reader.

Lemma 4.4 *Let $a \in GL_m(K)$, $b \in GL_n(K)$, and $x \in M_{mn}(K)$. If either $ax = 0$, or $xb = 0$, or $axb = 0$, then $x = 0$. So the map $y \mapsto ayb$ on $M_{mn}(K)$ is invertible.*

Proposition 4.5 *Let $L = L_1 \otimes L_2 \otimes L_3$ be as above. For $a \in GL_m(K)$, $b \in GL_n(K)$, and $c \in GL_p(K)$ let $T(a, b, c) : L \longrightarrow L$ be the linear map defined by*

$$T(a, b, c)(x \otimes y \otimes z) = axb^{-1} \otimes byc^{-1} \otimes cza^{-1}.$$

Then

$$H = \{T(a, b, c) \mid (a, b, c) \in GL_m(K) \times GL_n(K) \times GL_p(K)\}$$

is a subgroup of $\Gamma^0(t)$.

Proof. It follows from Lemma 4.4 that $T(a,b,c)$ is an automorphism of L. It is also easy to see that $T(a,b,c)T(a_1,b_1,c_1)=T(aa_1,bb_1,cc_1)$ for any $a,\dots,c_1$. Therefore H is a subgroup of $S^0(L_1,L_2,L_3)$.

Let D, E, F, … be as above. The group $G=G_D\times G_E\times G_F=GL_m(K)\times GL_n(K)\times GL_p(K)$ preserves $\delta_D\in D\otimes D'$, when acting on $D\otimes D'$, according to Lemma 4.1. Similarly G preserves δ_E and δ_F, and so preserves $\delta_D\otimes\delta_E\otimes\delta_F$. As $\tau: N\longrightarrow L$ is a G-homomorphism and $t=\tau(\delta_D\otimes\delta_E\otimes\delta_F)$, we see that G preserves t.

It remains to note that the image of $(a,b,c)\in G_D\times G_E\times G_F$ in $GL(L)$ coincides with $T(a,b,c)$. So $T(a,b,c)$ preserves t for any a, b, and c, whence $H\le\Gamma^0(t)$. □

4.3 Structure of the full $\Gamma(t)$

The full isotropy group $\Gamma(t)$, where $t=\langle m,n,p\rangle$, may be larger than $\Gamma^0(t)$. However, the relations between $\Gamma(t)$ and $\Gamma^0(t)$ can be easily described. This is the aim of the present subsection.

In the rest of this section we assume that at least one of the numbers m, n, and p is different from 1. If this is the case, then at most one of the three spaces L_1, L_2, and L_3 is one-dimensional. So for any decomposable automorphism $\varphi\in S(L_1,L_2,L_3)$ the permutation of $\{L_1,L_2,L_3\}$, corresponding to φ, is uniquely determined, by Proposition 3.3.

First of all, we construct some elements of $\Gamma(t)$, not belonging to $\Gamma^0(t)$. For a permutation g of $\{L_1,L_2,L_3\}$ we define certain decomposable automorphism $\rho_g: L\longrightarrow L$ (however, ρ_g will be defined not for any triple (m,n,p)).

Suppose that $m=n$. Define $\rho_{(23)}: L\longrightarrow L$ by the formula $\rho_{(23)}(x\otimes y\otimes z)=x^t\otimes z^t\otimes y^t$. (Note that we use the same symbol t for the tensor $t=\langle m,n,p\rangle$ and the transpose map, but we hope this will not lead to a confusion). Note that $\rho_{(23)}$ is well-defined indeed, because the formula $x\mapsto x^t$ defines an isomorphism of the space $L_2=M_{np}=M_{mp}$ onto $L_3=M_{pm}$, and also this formula defines an isomorphism of L_3 onto L_2, and an automorphism of L_1. Observe next that $\rho^2_{(23)}=1(=\mathrm{id}_L)$, as $\rho^2_{(23)}(x\otimes y\otimes z)=\rho_{(23)}(\rho_{(23)}(x\otimes y\otimes z))=\rho_{(23)}(x^t\otimes z^t\otimes y^t)=(x^t)^t\otimes(y^t)^t\otimes(z^t)^t=x\otimes y\otimes z$. Finally, we have $\rho_{(23)}\in\Gamma(t)$, because

$$\rho_{(23)}(t)=\rho_{(23)}(\sum_{\substack{1\le i,j\le m\\ 1\le k\le p}} e_{ij}\otimes e_{jk}\otimes e_{ki})=\sum_{\substack{1\le i,j\le m\\ 1\le k\le p}} e_{ji}\otimes e_{ik}\otimes e_{kj}=t$$

(note that if we change names of indices in the latter sum by $i\longrightarrow j$, $j\longrightarrow i$, $k\longrightarrow k$, then we obtain the sum for t).

Similarly, if $m=p$ or $n=p$, then we may define $\rho_{(12)}$ and $\rho_{(13)}$ by formulae

$$\begin{aligned}\rho_{(12)}(x\otimes y\otimes z) &= y^t\otimes x^t\otimes z^t\,, \qquad \text{and}\\ \rho_{(13)}(x\otimes y\otimes z) &= z^t\otimes y^t\otimes x^t\,,\end{aligned}$$

respectively.

Next suppose that $m=n=p$. Then we define $\rho_{(123)}$ and $\rho_{(132)}$ by the formulae

$$\rho_{(123)}(x\otimes y\otimes z)=z\otimes x\otimes y,$$

resp.

$$\rho_{(132)}(x\otimes y\otimes z)=y\otimes z\otimes x.$$

Clearly, $\rho^2_{(123)} = \rho_{(132)}$ and $\rho^3_{(123)} = 1$. Also, it is easy to see that $\rho_{(123)} \in \Gamma(t)$.

Finally, for any triple m, n, p define $\rho_e = \mathrm{id}_L$.

Observe that the permutation of the factors L_1, L_2, and L_3, corresponding to ρ_g, is precisely g. Hence $\rho_g \neq 1$ if $g \neq 1$, and also $\rho_g \neq \rho_h$, if $g \neq h$.

Let Q be the set of all ρ_g, that are defined, for given m, n, and p. Thus,

$$Q = \begin{cases} \{\rho_e = 1\}, & \text{if } m \neq n \neq p \neq m, \\ \{1, \rho_{(23)}\}, & \text{if } m = n \neq p, \\ \{1, \rho_{(12)}\}, & \text{if } m = p \neq n, \\ \{1, \rho_{(13)}\}, & \text{if } n = p \neq m, \\ \{1, \rho_{(12)}, \rho_{(13)}, \rho_{(23)}, \rho_{(123)}, \rho_{(132)}\}, & \text{if } m = n = p. \end{cases}$$

Lemma 4.6 *For any m, n, and p the set Q is a subgroup of $\Gamma(t)$. Let $R \leq S_3$ be the group of all permutations of $\{L_1, L_2, L_3\}$, preserving dimensions. Then the rule $g \leftrightarrow \rho_g$ defines isomorphism $R \leftrightarrow Q$. Thus, $Q \cong S_3$, Z_2, or 1, when $|\{m,n,p\}| = 1$, 2, or 3, respectively.*

Proof. First suppose that m, n, and p are pairwise distinct. Then the numbers $\dim L_1 = mn$, $\dim L_2 = np$, and $\dim L_3 = pm$ are pairwise distinct also, whence $R = 1$. Thus, in this case both Q and R are trivial groups, and the statement is trivial too.

Further suppose that $|\{m,n,p\}| = 2$. We consider, as an example, the case $m = n \neq p$ only. In this case $Q = \{\rho_e = 1, \rho_{(23)}\}$. Moreover, $\dim L_1 \neq \dim L_2 = \dim L_3$, whence $R = \{e, (23)\}$. As $\rho^2_{(23)} = 1$ and $\rho_{(23)} \neq 1$, we see that Q is a group isomorphic to Z_2, and that the bijection $e \leftrightarrow \rho_e = 1$, $(23) \leftrightarrow \rho_{(23)}$ is an isomorphism between R and Q.

Finally consider the case $m = n = p$. In this case $mn = np = pm$, whence $R \cong S_3$ consists of all permutations of $\{L_1, L_2, L_3\}$. Moreover, all ρ_g are pairwise distinct, and any ρ_g is an automorphism of L. So it is sufficient to prove that $\rho_g\rho_h = \rho_{gh}$ for each pair of $g, h \in S_3$.

It is not hard to check the latter equality in all cases directly. If $g = e$ or $h = e$, then this equality is trivial, as $\rho_e = 1$. It remains to check this equality for 25 pairs (g,h) with $g, h \neq e$, which is not too many.

There is, however, a shorter argument. For $g \in S_3$ let π_g be the usual permutation of factors, for example $\pi_{(13)}(x \otimes y \otimes z) = z \otimes y \otimes x$. Then $\pi_g\pi_h = \pi_{gh}$ for any g and h. Next, let $\tau : L \longrightarrow L$ be the componentwise transpose map, i.e., $\tau(x \otimes y \otimes z) = x^t \otimes y^t \otimes z^t$. Note that τ commutes with all π_g, and also that $\tau^2 = 1$. Next, note that $\rho_g = \pi_g$ if g is even, and $\rho_g = \tau\pi_g$ if g is odd. In other words, $\rho_g = \pi_g\tau^{\varepsilon(g)}$, where $\varepsilon : S_3 \longrightarrow Z_2 = \{0, 1\}$ is the parity homomorphism. Now for any g and h we have $\rho_g\rho_h = \pi_g\tau^{\varepsilon(g)}\pi_h\tau^{\varepsilon(h)} = \pi_g\pi_h\tau^{\varepsilon(g)}\tau^{\varepsilon(h)} = \pi_{gh}\tau^{\varepsilon(g)+\varepsilon(h)} = \pi_{gh}\tau^{\varepsilon(gh)} = \rho_{gh}$, as required. □

To state the next proposition it is convenient to use the notion of semidirect product.

Recall that a group G is the *product* of its subgroups A and B, which is denoted by $G = AB$, if for each $g \in G$ there exist $a \in A$ and $b \in B$ such that $g = ab$. If in addition $A \cap B = 1$, then it is easy to see that the representation of g in the form $g = ab$ is unique.

A group G is said to be a *semidirect product* of A by B, which is denoted by $G = A \leftthreetimes B$, if $G = AB$, A is normal in G, and $A \cap B = 1$.

Proposition 4.7 *Let $t = \langle m, n, p \rangle$, and let $Q \leq \Gamma(t)$ be the subgroup described above. Then $\Gamma(t) = \Gamma^0(t) \leftthreetimes Q$.*

Proof. We know that $\Gamma^0(t) \trianglelefteq \Gamma(t)$. Further, $Q \cap \Gamma^0(t) = 1$, because a nontrivial element of Q corresponds to a nontrivial permutation of L_1, L_2, L_3. It remains to show that $\Gamma(t) = \Gamma^0(t)Q$. Let $x \in \Gamma(t)$, and let g be the permutation of L_1, L_2, L_3, corresponding to x. Then g preserves the dimensions of factors, and therefore ρ_g is well-defined and $\rho_g \in Q$. Since the permutation of factors, corresponding to ρ_g, is g, it follows that the permutation of factors, corresponding to the element $x' = x\rho_g^{-1}$, is trivial, that is, $x' \in \Gamma^0(t)$. Thus, we have $x = x'\rho_g$, where $x' \in \Gamma^0(t)$ and $\rho_g \in Q$. Hence $\Gamma(t) = \Gamma^0(t)Q$. □

Proposition 4.8 *Let $T(a,b,c)$ and H be the transformations and the group introduced in Proposition 4.5. Then any element $g \in \Gamma^0(t)$ has the form $g = T(a,b,c)$, for some a, b, and c. Therefore, $\Gamma^0(t) = H$.*

This proposition will be proved later in this section.

Next we describe the group $\Gamma^0(t)$ as an abstract group.

Recall that the *projective general linear group $PGL_n(K)$* is the quotient group

$$PGL_n(K) = GL_n(K)/Z_n(K),$$

where $Z_n(K) = \{\lambda E_n \mid \lambda \in K^*\}$ is the subgroup of all nonzero scalar matrices.

(For reader's information we recall the following standard facts on linear groups; they can be found in many textbooks, see for instance [17] (§§I.1, I.2, II.1, II.2), [28] (§13), and [43](§I.9).

The group $Z_n(K)$ is the center of $GL_n(K)$. The group $PGL_n(K)$ contains the projective special linear group $PSL_n(K) = SL_n(K)/(Z_n(K) \cap SL_n(K))$ as a normal subgroup. The latter group is simple, except for the two cases $(n,K) = (2,\mathbb{F}_2)$, $(2,\mathbb{F}_3)$. The quotient $PGL_n(K)/PSL_n(K)$ is trivial, if K is algebraically closed, and is a finite cyclic group if K is finite.)

Let $\varphi : GL_m(K) \times GL_n(K) \times GL_p(K) \longrightarrow \Gamma^0(t)$ be the map defined by $\varphi((a,b,c)) = T(a,b,c)$. It was observed in the proof of Proposition 4.5 that φ is a group homomorphism. Proposition 4.8 shows that φ is surjective. Therefore, in order to describe its image $\operatorname{Im}\varphi = H = \Gamma^0(t)$ (as an abstract group, i.e., up to isomorphism), it is sufficient to know $\operatorname{Ker}\varphi$, its kernel.

We need a lemma.

Lemma 4.9 *Suppose $A \in GL_m(K)$ and $B \in GL_n(K)$ be matrices such that AxB is proportional to x for all matrices $x \in M_{mn}(K)$. Then A and B are scalar matrices.*

Proof. Consider the map $\alpha : x \mapsto AxB$ of $M_{mn}(K)$ to itself. It follows from Lemma 4.4 that α is an isomorphism. So α is a scalar map by Lemma 3.1 : $AxB = cx$, for a fixed $c \in K^*$. Next, let a_{ij} and b_{ij} be the coefficients of A and B, respectively:

$$A = \sum_{i,j=1}^{m} a_{ij}e_{ij}\,, \quad B = \sum_{i,j=1}^{n} b_{ij}e_{ij}\,.$$

Then for all p and q such that $1 \le p \le m$ and $1 \le q \le n$ we have

$$ce_{pq} = Ae_{pq}B = \sum_{1\le i\le m,\ 1\le j\le n} a_{ip}b_{qj}e_{ij}\,,$$

whence $a_{pp}b_{qq}=c$, and $a_{ip}b_{qj}=0$ if $i\neq p$ or $j\neq q$. The former of these relations implies that $a_{pp},b_{qq}\neq 0$ for all p and q. Taking $i=p$, $j\neq q$ in the second relation, we obtain $a_{pp}b_{qj}=0$, whence $b_{qj}=0$. Similarly, we obtain $a_{ip}=0$ for $i\neq p$. Thus, A and B are diagonal matrices. Next, for any q we have $a_{11}b_{qq}=c$, whence $b_{qq}=c/a_{11}$, so B is a scalar matrix. Similarly, A is a scalar matrix also. □

Proposition 4.10 *The kernel* $\operatorname{Ker}\varphi$ *coincides with* $Z_m(K)\times Z_n(K)\times Z_p(K)$*, and therefore the group* $\Gamma^0(t)=H$ *is isomorphic to* $PGL_m(K)\times PGL_n(K)\times PGL_p(K)$*.*

Proof. Let $(a,b,c)=(\lambda E_m,\mu E_n,\nu E_p)$, where $\lambda,\mu,\nu\in K^*$, be an element of $N=Z_m(K)\times Z_n(K)\times Z_p(K)$. Then for any $x\in L_1$, $y\in L_2$ and $z\in L_3$ we have

$$T(a,b,c)(x\otimes y\otimes z)=\lambda x\mu^{-1}\otimes\mu y\nu^{-1}\otimes\nu z\lambda^{-1}=x\otimes y\otimes z,$$

so $T(a,b,c)=1$. Hence $N\leq\operatorname{Ker}\varphi$.

Conversely, suppose that $(a,b,c)\in\operatorname{Ker}\varphi$. Then $T(a,b,c)(x\otimes y\otimes z)=x\otimes y\otimes z$ for all x, y, z, that is, $axb^{-1}\otimes byc^{-1}\otimes cza^{-1}=x\otimes y\otimes z$. Hence axb^{-1} is proportional to x by Lemma 3.2. So both a and b are scalar matrices by Lemma 4.9. The matrix c is scalar also by a similar argument, whence $(a,b,c)\in N$. Therefore $\operatorname{Ker}\varphi\leq N$. □

It may be useful to have explicit formulae for conjugation of an element of H by an element of Q (however, we will not use these formulae in the present work).

For a matrix $x\in GL_l(K)$ we denote by $x^\vee$ the matrix $x^\vee=(x^t)^{-1}=(x^{-1})^t$ (which is usually called the matrix *contragradient* to x).

Proposition 4.11 *The following relations hold:*

$$\rho_e T(a,b,c)\rho_e^{-1}=T(a,b,c),$$

$$\rho_{(12)}T(a,b,c)\rho_{(12)}^{-1}\ (=\rho_{(12)}T(a,b,c)\rho_{(12)})\ =T(c^\vee,b^\vee,a^\vee),$$

$$\rho_{(13)}T(a,b,c)\rho_{(13)}=T(a^\vee,c^\vee,b^\vee),$$

$$\rho_{(23)}T(a,b,c)\rho_{(23)}=T(b^\vee,a^\vee,c^\vee),$$

$$\rho_{(123)}T(a,b,c)\rho_{(123)}^{-1}=T(c,a,b),$$

$$\rho_{(132)}T(a,b,c)\rho_{(132)}^{-1}=T(b,c,a).$$

Proof. The first relation is trivial, because $\rho_e=1$. Prove the next relation, as an example. Note that $\rho_{(12)}^{-1}=\rho_{(12)}$, as $\rho_{(12)}^2=1$.

For $x\in L_1$, $y\in L_2$, and $z\in L_3$ we have $\rho_{(12)}(x\otimes y\otimes z)=y^t\otimes x^t\otimes z^t$, whence

$$\begin{aligned}x\otimes y\otimes z\quad&\overset{\rho_{(12)}}{\mapsto}y^t\otimes x^t\otimes z^t\overset{T(a,b,c)}{\mapsto}ay^tb^{-1}\otimes bx^tc^{-1}\otimes cz^ta^{-1}\\&\overset{\rho_{(12)}}{\mapsto}(bx^tc^{-1})^t\otimes(ay^tb^{-1})^t\otimes(cz^ta^{-1})^t=(c^{-1})^txb^t\otimes(b^{-1})^tya^t\otimes(a^{-1})^tzc^t\\&=c^\vee x(b^\vee)^{-1}\otimes b^\vee y(a^\vee)^{-1}\otimes a^\vee z(c^\vee)^{-1}=T(c^\vee,b^\vee,a^\vee)(x\otimes y\otimes z),\end{aligned}$$

whence

$$\rho_{(12)}T(a,b,c)\rho_{(12)}=T(c^\vee,b^\vee,a^\vee).$$

The other relations can be proved similarly. □

We summarize the results of this section in the following theorem. For the convenience of the future usage, we state this theorem "in full".

Theorem 4.12 *Let $m, n, p \in \mathbb{N}$, $(m, n, p) \neq (1, 1, 1)$, let $L_1 = M_{mn} = M_{mn}(K)$, $L_2 = M_{np}$, $L_3 = M_{pm}$, let $L = L_1 \otimes L_2 \otimes L_3$, and let*

$$t = \langle m, n, p\rangle = \sum_{1\le i\le m,\ 1\le j\le n,\ 1\le k\le p} e_{ij} \otimes e_{jk} \otimes e_{ki} \in L.$$

For elements $a \in GL_m(K)$, $b \in GL_n(K)$, $c \in GL_p(K)$ define transformation $T(a, b, c) : L \longrightarrow L$ by the formula

$$T(a, b, c)(x \otimes y \otimes z) = axb^{-1} \otimes byc^{-1} \otimes cza^{-1}.$$

Put

$$H = \{T(a, b, c) \mid (a, b, c) \in GL_m(K) \times GL_n(K) \times GL_p(K)\}.$$

Then $\Gamma^0(t) = H$. The transformations $T(a, b, c)$ and $T(a_1, b_1, c_1)$ coincide if and only if $a_1 = \lambda a$, $b_1 = \mu b$, and $c_1 = \nu c$, for some $\lambda, \mu, \nu \in K^*$. The group H is isomorphic to $PGL_m(K) \times PGL_n(K) \times PGL_p(K)$.

For any element $g \in S_3$ and some m, n, p define transformation $\rho_g : L \longrightarrow L$ as follows:
$\rho_e = 1 = \mathrm{id}_L$, for any m, n, p;
$\rho_{(23)}(x \otimes y \otimes z) = x^t \otimes z^t \otimes y^t$, when $m = n$;
$\rho_{(13)}(x \otimes y \otimes z) = z^t \otimes y^t \otimes x^t$, when $n = p$;
$\rho_{(12)}(x \otimes y \otimes z) = y^t \otimes x^t \otimes z^t$, when $m = p$;
$\rho_{(123)}(x \otimes y \otimes z) = z \otimes x \otimes y$ and $\rho_{(132)}(x \otimes y \otimes z) = y \otimes z \otimes x$, when $m = n = p$.

Put

$$Q = \{\rho_g \mid g \in S_3\,,\ \rho_g \text{ is well-defined}\}.$$

In other words,

$$Q = \begin{cases} \{\rho_e = 1\}, & \text{if } m \neq n \neq p \neq m, \\ \{1, \rho_{(23)}\}, & \text{if } m = n \neq p, \\ \{1, \rho_{(12)}\}, & \text{if } m = p \neq n, \\ \{1, \rho_{(13)}\}, & \text{if } n = p \neq m, \\ \{1, \rho_{(12)}, \rho_{(13)}, \rho_{(23)}, \rho_{(123)}, \rho_{(132)}\}, & \text{if } m = n = p. \end{cases}$$

Then Q is a subgroup of $\Gamma(t)$, isomorphic to S_3, Z_2, or 1, when $|\{m, n, p\}| = 1$, 2, or 3, respectively.

The group $\Gamma(t)$ is a semidirect product of $\Gamma^0(t)$ and Q:

$$\Gamma(t) = \Gamma^0(t) \leftthreetimes Q.$$

The following relations, describing action of Q on H by conjugation, hold (in all cases where ρ_g is well-defined):

$$\rho_e T(a, b, c)\rho_e^{-1} = T(a, b, c),$$

$$\rho_{(12)}T(a,b,c)\rho_{(12)}^{-1} \ (= \rho_{(12)}T(a,b,c)\rho_{(12)}) \ = T(c^\vee, b^\vee, a^\vee),$$
$$\rho_{(13)}T(a,b,c)\rho_{(13)} = T(a^\vee, c^\vee, b^\vee),$$
$$\rho_{(23)}T(a,b,c)\rho_{(23)} = T(b^\vee, a^\vee, c^\vee),$$
$$\rho_{(123)}T(a,b,c)\rho_{(123)}^{-1} = T(c,a,b),$$
$$\rho_{(132)}T(a,b,c)\rho_{(132)}^{-1} = T(b,c,a).$$

This theorem is an immediate consequence of Propositions 4.5, 4.8, 4.7, 4.10, and 4.11.

The aim of the rest of this section is to prove Proposition 4.8.

4.4 Structure tensors and contragradient maps

In this subsection we recall some well-known notions.

Let V be a space and V^* be its dual. For two elements $v \in V$ and $l \in V^*$ it will be convenient to denote $l(v)$ either by $\langle l, v\rangle$ or by $\langle v, l\rangle$. Thus, the element $\langle u_1, u_2\rangle$ is defined, if one of elements u_1 and u_2 is in V, the other is in V^*; and we always have $\langle u_1, u_2\rangle = \langle u_2, u_1\rangle$. The symbol $\langle u_1, u_2\rangle$ is called the *pairing* of u_1 and u_2.

Let $f : X \longrightarrow Y$ be a linear map. The map $f^* : Y^* \longrightarrow X^*$, taking an element $l \in Y^*$ to the element $m = f^*(l) \in X^*$, defined by $m(x) = l(f(x))$, is linear and is called the map, *dual* to f. Thus, f^* is the unique map such that

$$\langle l, f(x)\rangle = \langle f^*(l), x\rangle, \qquad \forall\, x \in X\,,\ l \in Y^*.$$

For any two maps $f : X \longrightarrow Y$ and $g : Y \longrightarrow Z$ the equality $(gf)^* = f^*g^*$ holds.

Suppose $f : X \longrightarrow Y$ is an isomorphism. It is easy to see that $f^* : Y^* \longrightarrow X^*$ is an isomorphism also. The inverse isomorphism $(f^*)^{-1} : X^* \longrightarrow Y^*$ is called an isomorphism, *contragradient* to f, and is denoted by $\check{f}$ or $f^\dagger$. It will be convenient for us to denote it by $f^\vee$. This isomorphism can be described as the unique isomorphism $f^\vee : X^* \longrightarrow Y^*$ such that

$$\langle f^\vee(l), f(x)\rangle = \langle l, x\rangle \quad \forall\, x \in X,\ l \in X^*.$$

It is easy to see that $(gf)^\vee = g^\vee f^\vee$ for any two isomorphisms $f : X \longrightarrow Y$ and $g : Y \longrightarrow Z$. Also, $(f^{-1})^\vee = (f^\vee)^{-1}$. In particular, suppose that $\varphi : G \longrightarrow GL(X)$ is a representation of a group G on a space X. Then the map $\varphi^* : G \longrightarrow GL(X^*)$, defined by $\varphi^*(g) = \varphi(g)^\vee$, is a representation of G also. It is called a representation *contragradient* (or more often *dual*) to φ. (Thus, the usage of the word "dual" for linear maps and for group representations is somewhat different).

Finally note that taking contragradient map is involutive, that is, $(f^\vee)^\vee = f$ for any isomorphism $f : X \longrightarrow Y$. (Strictly speaking, $(f^\vee)^\vee$ is a map from $(X^*)^*$ to $(Y^*)^*$, but we can identify $(V^*)^*$ with V, because we consider only finite-dimensional spaces.)

Let X, Y, Z be spaces. By $\mathcal{L}(X,Y)$ we denote the space of all linear maps from X to Y, and by $\mathcal{L}_2(X,Y;Z)$ the space of all bilinear maps $f : X \times Y \longrightarrow Z$. The spaces $\mathcal{L}(X,Y)$ and $\mathcal{L}_2(X,Y;Z)$ may be identified, in a canonical way, with $X^* \otimes Y$ and $X^* \otimes Y^* \otimes Z$, respectively (see [32], §4.2). Recall the description of this identification. Let $l \in X^*$ and $y \in Y$. Consider the map $\varphi_{l,y} : X \longrightarrow Y$, defined by

$$\varphi_{l,y}(x) = l(x)y.$$

Clearly, $\varphi_{l,y}$ is a linear map. Furthermore, the expression $l(x)y$ is linear in all three arguments l, x, and y, and therefore the rule $(l, y) \mapsto \varphi_{l,y}$ defines a bilinear map from $X^* \times Y$ to $\mathcal{L}(X, Y)$. By the universal property of tensor product there exists a unique linear map $\varphi : X^* \otimes Y \longrightarrow \mathcal{L}(X, Y)$ such that $\varphi(l \otimes y) = \varphi_{l,y}$ for all l and y.

Show that this φ is an isomorphism. Let $e_1, \dots, e_m$ and $f_1, \dots, f_n$ be bases of X and Y, respectively, and $e^1, \dots, e^m$ be the basis of X^* dual to (e_i). Then $\{e^i \otimes f_j \mid 1 \le i \le m,\ 1 \le j \le n\}$ is a basis of $X^* \otimes Y$. Put $h_{ij} = \varphi(e^i \otimes f_j)$. It is easy to see that h_{ij} is the linear map that takes e_i to f_j and takes e_l to 0 for all $l \ne i$. Clearly, $\{h_{ij} \mid i, j\}$ is a basis of $\mathcal{L}(X, Y)$. Thus, φ takes a basis of $X^* \otimes Y$ to a basis of $\mathcal{L}(X, Y)$, and is therefore an isomorphism. The map φ is called the *canonical isomorphism* between $X^* \otimes Y$ and $\mathcal{L}(X, Y)$.

We can define the isomorphism $\varphi : X^* \otimes Y^* \otimes Z \longrightarrow \mathcal{L}_2(X, Y; Z)$ in a similar way. Namely, φ is the unique linear map such that

$$(\varphi(l \otimes m \otimes z))(x, y) = l(x)m(y)z \quad \forall\, x \in X,\ y \in Y, z \in Z,\ l \in X^*,\ m \in Y^*$$

(the details are left to the reader).

Let $f \in \mathcal{L}(X, Y)$ (resp., $f \in \mathcal{L}_2(X, Y; Z)$), and let $h \in X^* \otimes Y$ (resp., $h \in X^* \otimes Y^* \otimes Z$) be a tensor such that $\varphi(h) = f$. This h is called the *structure tensor* of f, and will be denoted by $\widetilde{f}$.

Consider the group $G = GL(X) \times GL(Y)$. It acts on the spaces $X^* \otimes Y$ and $\mathcal{L}(X, Y)$ as usually. That is, an element $g = (g_1, g_2) \in G$ acts on $X^* \otimes Y$ as $g_1^\vee \otimes g_2$, and the action of g on $\mathcal{L}(X, Y)$ is defined by $g(f) = g_2 f g_1^{-1}$ (we leave to the reader to show that this is indeed a left action). Similarly, the group $G = GL(X) \times GL(Y) \times GL(Z)$ acts on $X^* \otimes Y^* \otimes Z$ and on $\mathcal{L}_2(X, Y; Z)$. The element $g = (g_1, g_2, g_3) \in G$ acts on $X^* \otimes Y^* \otimes Z$ as $g_1^\vee \otimes g_2^\vee \otimes g_3$, and the action on $\mathcal{L}_2(X, Y; Z)$ is described by the rule

$$(g(f))(x, y) = g_3(f(g_1^{-1}(x), g_2^{-1}(y)))$$

(i.e., g takes f to the map f_1 defined by $f_1(x, y) = g_3(f(g_1^{-1}(x), g_2^{-1}(y)))$; we may also write this as $g(f) = g_3 \circ f \circ (g_1^{-1} \times g_2^{-1})$).

Proposition 4.13 *Let $G = GL(X) \times GL(Y)$ (resp. $G = GL(X) \times GL(Y) \times GL(Z)$), and let $\varphi : X^* \otimes Y \longrightarrow \mathcal{L}(X, Y)$ (resp. $\varphi : X^* \otimes Y^* \otimes Z \longrightarrow \mathcal{L}_2(X, Y; Z)$) be the canonical isomorphism. Then φ is an isomorphism of KG-modules.*

Proof. It was observed above that φ is an isomorphism of vector spaces. By the observation preceding Lemma 4.3 it is sufficient to check that φ is a homomorphism of KG-modules. We prove this statement only for $\varphi : X^* \otimes Y \longrightarrow \mathcal{L}(X, Y)$, leaving the second statement to the reader.

We have to check that $g(\varphi(u)) = \varphi(g(u))$ for all $g = (g_1, g_2) \in G$ and $u \in X^* \otimes Y$. By linearity, we may assume that $u = l \otimes y$. The condition $g(\varphi(u)) = \varphi(g(u))$ means that $(g(\varphi(u)))(x) = (\varphi(g(u)))(x)$ for all $x \in X$. Thus, we have to show that

$$((g_1, g_2)(\varphi(l \otimes y)))(x) = (\varphi((g_1, g_2)(l \otimes y)))(x) \tag{3}$$

for all $g_1 \in GL(X)$, $g_2 \in GL(Y)$, $l \in X^*$, $y \in Y$, and $x \in X$.

We have $((g_1, g_2)(\varphi(l \otimes y)))(x) = ((g_1, g_2)(\varphi_{l,y}))(x)$ (by the definition of φ) $= g_2(\varphi_{l,y}(g_1^{-1}x))$ (by the definition of the action of G on $\mathcal{L}(X, Y)$) $= g_2(l(g_1^{-1}x)y)$ (by the definition of $\varphi_{l,y}$) $= l(g_1^{-1}x)g_2(y)$ (because g_2 is linear, and $l(g_1^{-1}x)$ is an element of K).

On the other hand, $(\varphi((g_1, g_2)(l \otimes y)))(x) = (\varphi(g_1^{\vee}l \otimes g_2y))(x)$ (by the definition of the action of G on $X^* \otimes Y$) $= \varphi_{g_1^{\vee}l, g_2y}(x)$ (by the definition of φ) $= (g_1^{\vee}l)(x) \cdot g_2y$ (by the definition of $\varphi_{l,y}$). Further, note that $(g_1^{\vee}l)(x) = \langle g_1^{\vee}l, x\rangle = \langle g_1^{\vee}l, g_1(g_1^{-1}x)\rangle$ (as $x = g_1(g_1^{-1}x)$) $= \langle l, g_1^{-1}x\rangle$ (by the property of contragradient maps) $= l(g_1^{-1}x)$. Hence $(g_1^{\vee}l)(x) \cdot g_2y = l(g_1^{-1}x) \cdot g_2y$.

Thus, both the left-hand and right-hand sides of (3) are equal to $l(g_1^{-1}x) \cdot g_2y$, and therefore (3) is true. □

4.5 The isotropy group of a bilinear map

Let X, Y, and Z be vector spaces and let $f \in \mathcal{L}_2(X, Y; Z)$ be a bilinear map. The group $G = GL(X) \times GL(Y) \times GL(Z)$ acts on $\mathcal{L}_2(X, Y; Z)$ in the way described in the previous subsection. The stabilizer of f in G with respect to this action will be called the *isotropy group* of f, and will be denoted by $\Delta(f)$. The reader can easily check that this definition is equivalent to the following: $\Delta(f)$ is the set of all triples $(A, B, C) \in G$ such that $f(Ax, By) = Cf(x, y)$ for all $x \in X$ and $y \in Y$. In other words, the diagram

$$\begin{tikzcd}
X \times Y \arrow[r, "f"] \arrow[d, "A\times B"'] & Z \arrow[d, "C"] \\
X \times Y \arrow[r, "f"] & Z
\end{tikzcd}$$

must commute.

Example. Let X, Y, and Z be three spaces, let $U = \mathcal{L}(X, Y)$, $V = \mathcal{L}(Y, Z)$, $W = \mathcal{L}(X, Z)$, and let $f : U \times V \to W$ be the usual composition of mappings, i.e., $f(x, y) = yx$. Clearly f is bilinear. For $g = (g_1, g_2, g_3) \in GL(X) \times GL(Y) \times GL(Z)$ put $R(g) = (A, B, C)$, where $A : U \to U$, $B : V \to V$, and $C : W \to W$ are defined by the rules $Ax = g_2xg_1^{-1}$, $Bx = g_3xg_2^{-1}$, and $Cx = g_3xg_1^{-1}$, respectively. Then it is easy to see that $R(g) \in \Delta(f)$ for all g. Moreover, $R : g \mapsto R(g)$ is a group homomorphism. Later we will show that R is an *epimorphism.*

The following proposition shows that the isotropy group of a bilinear map is closely related to the (small) isotropy group of the structure tensor of this map.

Proposition 4.14 *Let $f : X \times Y \to Z$ be a bilinear map and let $\widetilde{f} \in X^* \otimes Y^* \otimes Z$ be its structure tensor. Let $(A, B, C) \in GL(X) \times GL(Y) \times GL(Z)$. Then $(A, B, C) \in \Delta(f)$ if and only if $A^{\vee} \otimes B^{\vee} \otimes C \in \Gamma^0(\widetilde{f})$.*

Proof. By Proposition 4.13, the map $h \mapsto \widetilde{h}$ is a G-isomorphism from $\mathcal{L}_2(X, Y; Z)$ to $X^* \otimes Y^* \otimes Z$, where $G = GL(X) \times GL(Y) \times GL(Z)$. So $g = (A, B, C) \in G$ is in $\Delta(f)$ if and only if g fixes $\widetilde{f}$. But $g(\widetilde{f}) = (A^{\vee} \otimes B^{\vee} \otimes C)\widetilde{f}$ by the definition of the action of G on $X^* \otimes Y^* \otimes Z$. □

4.6 Type of a space of linear maps

Let X and Y be vector spaces, $\dim X = m$ and $\dim Y = n$. Let $\mathcal{L} = \mathcal{L}(X,Y)$, and $L \subseteq \mathcal{L}$ be some space of linear maps from X to Y. It is natural to call spaces

$$\operatorname{Ker} L = \bigcap_{f\in L} \operatorname{Ker} f = \{x \in X \mid f(x) = 0 \ \ \forall\, f \in L\}$$

and

$$\operatorname{Im} L = \sum_{f\in L} \operatorname{Im} f$$

the *kernel* and *image* of L, respectively.

Put $\beta_1(L) = m - \dim \operatorname{Ker} L$ and $\beta_2(L) = \dim \operatorname{Im} L$. The pair $\beta(L) = (\beta_1(L), \beta_2(L))$ will be called the *type* of L.

Note that for any linear map $f \in \mathcal{L}(X,Y)$ we have $\dim \operatorname{Ker} f + \dim \operatorname{Im} f = m$, so for a one-dimensional subspace $\langle f\rangle \subseteq \mathcal{L}(X,Y)$ we have $\beta_1(\langle f\rangle) = \beta_2(\langle f\rangle) = \dim \operatorname{Im} f = \operatorname{rk}(f)$. Thus, $\beta(L)$ is a generalization of the rank of a linear map.

Let $f \in \mathcal{L}(X,Y)$, and let $a \in GL(X)$ and $b \in GL(Y)$ be automorphisms of X and Y, respectively. Then $bfa \in \mathcal{L}(X,Y)$. It is easy to see that

$$\operatorname{Ker} bfa = a^{-1}(\operatorname{Ker} f), \quad \text{and} \quad \operatorname{Im} bfa = b(\operatorname{Im} f).$$

Hence, if $\tau_{a,b} : \mathcal{L} \longrightarrow \mathcal{L}$ is a linear transformation defined by $\tau_{a,b}(f) = bfa$, then

$$\operatorname{Ker} \tau_{a,b}(L) = a^{-1}(\operatorname{Ker} L) \quad \text{and} \quad \operatorname{Im} \tau_{a,b}(L) = b(\operatorname{Im} L),$$

for any subspace $L \subseteq \mathcal{L}$. It follows that $\tau_{a,b}$ preserves the type:

$$\beta(\tau_{a,b}(L)) = \beta(L) \quad \forall\, L \subseteq \mathcal{L}.$$

The aim of this subsection is to prove the converse statement.

Proposition 4.15 *Let $\mathcal{L} = \mathcal{L}(X,Y)$, and let $h : \mathcal{L} \longrightarrow \mathcal{L}$ be a linear transformation such that $\beta(h(L)) = \beta(L)$ for all subspaces $L \subseteq \mathcal{L}$. Then there exist $a \in GL(X)$ and $b \in GL(Y)$ such that $h = \tau_{a,b}$.*

Proof. It is useful to observe that the set of all transformations of the form $\tau_{a,b}$ is a group, because $\tau_{a,b}\tau_{c,d} = \tau_{ac,bd}$, and $\tau_{\mathrm{id}_X,\mathrm{id}_Y} = \mathrm{id}_{\mathcal{L}(X,Y)}$, whence also $(\tau_{a,b})^{-1} = \tau_{a^{-1},b^{-1}}$. It is obvious that the group

$$\{\tau_{a,b} \mid a \in GL(X), b \in GL(Y)\}$$

is the image of $GL(X) \times GL(Y)$ under the representation of the latter group on $\mathcal{L}(X,Y)$, described in Subsection 4.4.

Take bases $(e_1, \dots, e_m)$ and $(d_1, \dots, d_n)$ of X and Y, respectively. Moreover, let $(e^1, \dots, e^m)$ be the basis of X^* dual to (e_i). Let $f_{ij} : X \longrightarrow Y$ be the map defined by $f_{ij}(e_i) = d_j$, $f_{ij}(e_l) = 0$ when $l \neq i$. Then $\{f_{ij} \mid 1 \le i \le m, 1 \le j \le n\}$ is a basis of $\mathcal{L}$. Moreover, $f_{ij} = \varphi_{e^i,d_j}$, where for $l \in X^*$ and $y \in Y$

$$\varphi_{l,y} = \varphi(l \otimes y) : x \mapsto l(x)y$$

is the linear map, described in Subsection 4.4.

It was noted above that $\beta(\langle f\rangle) = (\mathrm{rk}(f), \mathrm{rk}(f))$ for any $f \in \mathcal{L}(X,Y)$. So h preserves the rank: $\mathrm{rk}(h(f)) = \mathrm{rk}(f)$ for all $f \in \mathcal{L}$.

Put $q_{ij} = h(f_{ij})$. As f_{ij} are of rank 1, and $\{f_{ij}\}$ is a basis of $\mathcal{L}$, it follows that all q_{ij} are also of rank 1, and

$$\{q_{ij} \mid 1 \le i \le m,\ 1 \le j \le n\}$$

is a basis of $\mathcal{L}$.

It is easy to see that the maps $f \in \mathcal{L}$ of rank 1 are precisely the maps of the form $\varphi_{l,y}$. In particular, there exist $l_{ij} \in X^*$ and $y_{ij} \in Y$ such that $q_{ij} = \varphi_{l_{ij},y_{ij}}$ for all $1 \le i \le m$, $1 \le j \le n$.

Show that l_{i,j_1} and $l_{i,j_2} \in X^*$ are proportional, for any i, j_1, and j_2; in other words, the line $\langle l_{ij}\rangle \subseteq X^*$ depends only on i. Consider the space $L = \langle f_{i,j_1}, f_{i,j_2}\rangle$. Obviously, $\mathrm{Ker}\, L = \langle e_l \mid l \ne i\rangle$ has codimension 1 in X^*, so the kernel of $h(L) = \langle q_{i,j_1}, q_{i,j_2}\rangle$ must be of codimension 1 also. Now observe that $\mathrm{Ker}\,\varphi_{l,y} = \mathrm{Ker}\, l$ and $\mathrm{Im}\,\varphi_{l,y} = \langle y\rangle$, for any $l \in X^*$ and $y \in Y$ such that $l, y \ne 0$. In particular, $\mathrm{Ker}\, q_{ij} = \mathrm{Ker}\, l_{ij}$ and $\mathrm{Im}\, q_{ij} = \langle y_{ij}\rangle$, for all i and j. Hence $\mathrm{Ker}\,\langle q_{i,j_1}, q_{i,j_2}\rangle = \mathrm{Ker}\, l_{i,j_1} \cap \mathrm{Ker}\, l_{i,j_2}$. If l_{i,j_1} and l_{i,j_2} are not proportional, then the latter intersection is a subspace of codimension 2 in X^*, a contradiction. Thus, l_{i,j_1} and l_{i,j_2} are proportional. Therefore, there exist $l_1, \dots, l_m \in X^*$ such that $\langle l_{ij}\rangle = \langle l_i\rangle$, for all i and j.

Similarly, one can show that $\langle y_{ij}\rangle$ depends only on j. Indeed, for given $i_1 \ne i_2$, $1 \le i_1, i_2 \le m$, consider the space $L = \langle f_{i_1,j}, f_{i_2,j}\rangle$. Its image is $\langle d_j\rangle$. So the image of the space $\langle q_{i_1,j}, q_{i_2,j}\rangle = h(L)$ is of dimension 1 also, whence $\langle y_{i_1,j}\rangle = \langle y_{i_2,j}\rangle$, whence $\langle y_{ij}\rangle = \langle y_j\rangle$, for some $y_1, \dots, y_n \in Y$.

Thus, we see that $q_{ij} = \varphi_{l_{ij},y_{ij}} = \lambda_{ij}\varphi_{l_i,y_j}$, for some $\lambda_{ij} \in K^*$.

Show that $(y_1, \dots, y_n)$ is a basis of Y. Otherwise, $\langle y_1, \dots, y_n\rangle = Y'$ is a proper subspace of Y. But the image of any q_{ij} lies in Y', so the image of the whole $\mathcal{L}(X,Y) = \langle q_{ij} \mid 1 \le i \le m,\ 1 \le j \le n\rangle$ also lies in Y', which is impossible when $Y' \ne Y$.

Similarly, $(l_1, \dots, l_m)$ is a basis of X^*. Indeed, if this is not the case, then there exists an element $x \in X$, $x \ne 0$, annihilated by all q_{ij}, i.e., by the whole $\mathcal{L}(X,Y)$.

Further, we "normalize" basis $\{q_{ij}\}$ in an appropriate way. To do this, we need to know how $\tau_{a,b}$ acts on $\varphi_{l,y}$. Prove that

$$\tau_{a,b}(\varphi_{l,y}) = \varphi_{a^*(l),b(y)}\ , \tag{4}$$

where $a^* \in GL(X^*)$ is the map dual to a. Indeed, for all $x \in X$ we have $(\tau_{a,b}(\varphi_{l,y}))(x) = (b\varphi_{l,y}a)(x) = b(\varphi_{l,y}(a(x))) = b(l(a(x))y) = l(a(x))b(y)$. Since $l(a(x)) = (a^*(l))(x)$ by the definition of the dual map, we finally get

$$(\tau_{a,b}(\varphi_{l,y}))(x) = (a^*(l))(x)b(y) = \varphi_{a^*(l),b(y)}(x),$$

which proves formula (4). Let $b_1 \in GL(Y)$ be the element taking basis $(y_1, \dots, y_n)$ to $(d_1, \dots, d_n)$, let $c \in GL(X^*)$ takes $(l_1, \dots, l_m)$ to $(e^1, \dots, e^m)$, and $a_1 = c^* \in GL(X)$ be the map dual to c. Then τ_{a_1,b_1} takes φ_{l_i,y_j} to $\varphi_{a_1^*(l_i),b_1(y_j)} = \varphi_{e^i,d_j} = f_{ij}$. As $q_{ij} = \lambda_{ij}\varphi_{l_i,y_j}$, we see that the map $h' = \tau_{a_1,b_1}h$ takes f_{ij} to $\lambda_{ij}f_{ij}$. Moreover, h' preserves types of subspaces. Thus, it remains to show that a map h', taking f_{ij} to $\lambda_{ij}f_{ij}$, where $\lambda_{ij} \in K^*$, and preserving the types, must have the form $\tau_{a,b}$.

Multiplying h' by a scalar we may assume that $\lambda_{11} = 1$. Put $\mu_i = \lambda_{i1}$, $\nu_j = \lambda_{1j}$ (whence $\mu_1 = \nu_1 = 1$), and show that $\lambda_{ij} = \mu_i\nu_j$. This is evident if $i = 1$ or $j = 1$, so suppose $i, j > 1$. Consider $f = f_{11} + f_{i1} + f_{1j} + f_{ij} \in \mathcal{L}$, then $h'(f) = f_{11} + \mu_i f_{i1} + \nu_j f_{1j} + \lambda_{ij} f_{ij}$. As $\operatorname{rk}(f) = 1$, we must have $\operatorname{rk}(h'(f)) = 1$, which is the case only if $\lambda_{ij} = \mu_i\nu_j$.

Let a and b be the linear maps on X and Y such that $a(e_i) = \mu_i e_i$ and $b(d_j) = \nu_j d_j$. Then it is easy to see that $bf_{ij}a = \mu_i\nu_j f_{ij} = \lambda_{ij} f_{ij} = h'(f_{ij})$, for all i and j, and therefore $h' = \tau_{a,b}$. □

4.7 Further lemmas on linear maps

Lemma 4.16 *Let U and V be spaces, $f_1, \ldots, f_n : U \to V$ be linear maps such that $\cap_{i=1}^n \operatorname{Ker} f_i = 0$. Then for any linear function $l : U \to K$ there exist linear functions $l_i : V \to K$ such that $l = \sum_{i=1}^n l_i \circ f_i$.*

Proof. Let $T \subseteq U^*$ be the set of all linear functions of the form $\sum_{i=1}^n l_i \circ f_i$, for some $l_i \in V^*$. Clearly, $T \subseteq U^*$ is a subspace. To prove that $T = U^*$ it is sufficient to show that there is no a non-zero vector $u \in U$ such that $t(u) = 0$ for all $t \in T$.

Let $u \in U$, $u \neq 0$. As $\cap_{i=1}^n \operatorname{Ker} f_i = 0$, there exist i such that $f_i(u) \neq 0$. Next, there exist a linear function $m \in V^*$ such that $m(f_i(u)) \neq 0$. Then $m' = m \circ f_i \in T$ and $m'(u) = (m \circ f_i)(u) = m(f_i(u)) \neq 0$. □

Lemma 4.17 *Let U, V, and W be three spaces, $f_1 \ldots, f_n \in \mathcal{L}(U, V)$ and $f \in \mathcal{L}(U, W)$. Then f can be represented in the form $f = g_1 f_1 + \ldots + g_n f_n$, for some $g_i \in \mathcal{L}(V, W)$, if and only if $\cap_{i=1}^n \operatorname{Ker} f_i \subseteq \operatorname{Ker} f$.*

Proof. Denote $\cap_{i=1}^n \operatorname{Ker} f_i$ by S. It is clear that if f can be represented in the form $f = g_1 f_1 + \ldots + g_n f_n$, then $S \subseteq \operatorname{Ker} f$. We need to prove the converse implication.

First assume that $S = 0$ and $\dim W = 1$. Then we may identify W with K, so that f and g_i became linear functions on U and V, respectively, and the desired statement follows from Lemma 4.16.

Next consider the case when $S = 0$, but W may be of arbitrary dimension. Let $(w_1, \ldots, w_m)$ be a basis of W. Then f decomposes as

$$f = \sum_{j=1}^{m} f^{(j)},$$

where $f^{(j)} \in \mathcal{L}(U, \langle w_j \rangle)$. According to the case $S = 0$ and $\dim W = 1$, there exist linear maps $g_i^{(j)} : V \to \langle w_j \rangle$, where $1 \leq i \leq n$, $1 \leq j \leq m$, such that $f^{(j)} = \sum_{i=1}^n g_i^{(j)} f_i$ for all $j = 1, \ldots, m$. Now it is sufficient to take $g_i = \sum_{j=1}^m g_i^{(j)}$. Thus the case $S = 0$ is settled.

Finally consider the general case, when S may be nontrivial. Put $\overline{U} = U/S$, and let $\varphi : U \to \overline{U}$ be the canonical factorization mapping. As f and all f_i vanish on S, there exist unique maps $\overline{f} \in \mathcal{L}(\overline{U}, W)$ and $\overline{f}_i \in \mathcal{L}(\overline{U}, V)$ such that $f = \overline{f}\varphi$ and $f_i = \overline{f}_i\varphi$. It is clear that $\operatorname{Ker} \overline{f} = (\operatorname{Ker} f)/S$ and $\operatorname{Ker} \overline{f}_i = (\operatorname{Ker} f_i)/S$.

As $\cap_{i=1}^{n}\mathrm{Ker}\, f_i = S$, we have $\cap_{i=1}^{n}\mathrm{Ker}\,\overline{f}_i = 0$. Applying the previous case we see that $\overline{f} = \sum_{i=1}^{n} g_i\overline{f}_i$ for some linear maps $g_i : V \to W$. Hence

$$f = \overline{f}\varphi = (\sum_{i=1}^{n} g_i\overline{f}_i)\varphi = \sum_{i=1}^{n} g_i(\overline{f}_i\varphi) = \sum_{i=1}^{n} g_i f_i\,.$$

□

The next lemma is, in a sense, dual to the previous one.

Lemma 4.18 *Let U, V and W be three spaces, $f_1, \dots, f_n \in \mathcal{L}(V,W)$, and $f \in \mathcal{L}(U,W)$. Then f can be represented in the form $f = \sum_{i=1}^{n} f_i g_i$, for some $g_i \in \mathcal{L}(U,V)$, if and only if* $\mathrm{Im}\, f \subseteq \sum_{i=1}^{n} \mathrm{Im}\, f_i$.

Proof. Denote $\sum_{i=1}^{n} \mathrm{Im}\, f_i$ by S. It is clear that if f can be represented as $f = \sum_{i=1}^{n} f_i g_i$, then $\mathrm{Im}\, f \subseteq S$. Prove the converse implication. Suppose that $\mathrm{Im}\, f \subseteq S$. There exists a basis $w_1, \dots, w_m$ of S such that each w_j has the form $w_j = f_p(v_j)$, for some $p = p(j)$ and $v_j \in V$. Next, let $l_j : U \to K$ be the (uniquely defined) linear functions such that

$$f(u) = \sum_{j=1}^{m} l_j(u) w_j\,,$$

for all $u \in U$. Now for $j = 1, \dots, m$ define linear maps $h_j : U \to V$ by $h_j(u) = l_j(u)v_j$. Then

$$f(u) = \sum_{j=1}^{m} l_j(u)w_j = \sum_{j=1}^{m} l_j(u) f_{p(j)}(v_j) = \sum_{j=1}^{m} f_{p(j)}(l_j(u)v_j) = \sum_{j=1}^{m} f_{p(j)}(h_j(u)),$$

for all $u \in U$. That is, $f = \sum_{j=1}^{m} f_{p(j)} h_j$. But

$$\sum_{j=1}^{m} f_{p(j)} h_j = \sum_{i=1}^{n} f_i g_i\,,$$

where $g_i = \sum_{\{j|p(j)=i\}} h_j$. □

It is convenient to rewrite results of Lemmas 4.17 and 4.18 in a slightly different form, using the notions of kernel and image of a space of linear maps.

For subspaces $A \subseteq \mathcal{L}(U,V)$ and $B \subseteq \mathcal{L}(V,W)$ define subspace $BA \subseteq \mathcal{L}(U,W)$ by

$$BA = \langle ba \mid a \in A,\ b \in B\rangle.$$

In particular, we can consider subspaces $\mathcal{L}(V,W)A$ and $B\mathcal{L}(U,V)$ of $\mathcal{L}(U,W)$.

Proposition 4.19 *Let U, V, and W be three spaces, $A \subseteq \mathcal{L}(U,V)$ and $B \subseteq \mathcal{L}(V,W)$ be subspaces, and let $f \in \mathcal{L}(U,W)$. Then the following statements hold.*

1) $f \in \mathcal{L}(V,W)A$ if and only if $\mathrm{Ker}\, f \supseteq \mathrm{Ker}\, A$.

2) $f \in B\mathcal{L}(U,V)$ if and only if $\mathrm{Im}\, f \subseteq \mathrm{Im}\, B$.

We leave to the reader to deduce statements 1) and 2) from Lemmas 4.17 and 4.18, respectively.

4.8 The isotropy group of the map of composition of linear maps

Let U, V and W be three vector spaces, and let

$$\varphi : \mathcal{L}(U,V) \times \mathcal{L}(V,W) \to \mathcal{L}(U,W)$$

be the usual composition of mappings, i.e., $\varphi(x,y) = yx$. The aim of the present subsection is to find the isotropy group $\Delta(\varphi)$.

For subspaces $A \subseteq \mathcal{L}(U,V)$ and $B \subseteq \mathcal{L}(V,W)$ we define their *annihilators* by

$$\operatorname{ann}(A) = \{h \in \mathcal{L}(V,W) \mid hA = 0\}$$

and

$$\operatorname{ann}(B) = \{h \in \mathcal{L}(U,V) \mid Bh = 0\},$$

respectively.

For a subspace $L \subseteq \mathcal{L}(U,V)$ or $L \subseteq \mathcal{L}(V,W)$ let $\beta(L) = (\beta_1(L), \beta_2(L))$ be its type, as described in Subsection 4.6.

We need a lemma.

Lemma 4.20 *For subspaces $A \subseteq \mathcal{L}(U,V)$ and $B \subseteq \mathcal{L}(V,W)$ the following equalities hold:*
(1) $\dim \mathcal{L}(V,W)A = \beta_1(A) \dim W$*;*
(2) $\dim \operatorname{ann}(A) = (\dim V - \beta_2(A)) \dim W$*;*
(3) $\dim B\mathcal{L}(U,V) = \beta_2(B) \dim U$*;*
(4) $\dim \operatorname{ann}(B) = (\dim V - \beta_1(B)) \dim U$*.*

Proof. (1) Let $S = \operatorname{Ker} A$. By statement 1) of Proposition 4.19 $\mathcal{L}(V,W)A$ consists of all $h \in \mathcal{L}(U,W)$ such that $h(S) = 0$. Hence $\dim \mathcal{L}(V,W)A = (\dim U - \dim S) \dim W = \beta_1(A) \dim W$.

(2) Let $T = \operatorname{Im} A$. Consider $f \in \mathcal{L}(V,W)$. If $f(T) = 0$, then $fA = 0$, that is, $f \in \operatorname{ann}(A)$. On the other hand, if $f(T) \neq 0$, then there exist $u \in U$ and $h \in A$ such that $f(h(u)) \neq 0$, whence $(fh)(u) \neq 0$, and therefore $fh \neq 0$ and $f \notin \operatorname{ann}(A)$. Thus, $f \in \operatorname{ann}(A)$ if and only if $f(T) = 0$. Hence $\dim \operatorname{ann}(A) = (\dim V - \dim T) \dim W = (\dim V - \beta_2(A)) \dim W$.

(3) Let $T = \operatorname{Im} B$. By statement 2) of Proposition 4.19 an element $f \in \mathcal{L}(U,W)$ is in $B\mathcal{L}(U,V)$ if and only if $\operatorname{Im} f \subseteq T$, whence $B\mathcal{L}(U,V) = \mathcal{L}(U,T)$, and therefore $\dim B\mathcal{L}(U,V) = (\dim U)(\dim T) = (\dim U)\beta_2(B)$.

(4) It is easy to see that $\operatorname{ann}(B)$ consists of all $f \in \mathcal{L}(U,V)$ such that $\operatorname{Im} f \subseteq \operatorname{Ker} B$. Hence $\operatorname{ann}(B) = \mathcal{L}(U, \operatorname{Ker} B)$ and $\dim \operatorname{ann}(B) = (\dim U)(\dim \operatorname{Ker} B) = (\dim V - \beta_1(B)) \dim U$. □

We also need the following lemma, whose proof is left to the reader.

Lemma 4.21 *Let U, V, and W be three spaces, and let $a, b \in \mathcal{L}(V,V)$ be maps such that $yax = ybx$ for all $x \in \mathcal{L}(U,V)$ and $y \in \mathcal{L}(V,W)$. Then $a = b$.*

Recall that the center of the group $GL(V)$ consists of scalar transformations, for any V, see the remark after Proposition 4.8.

Proposition 4.22 *Let X, Y and Z be vector spaces, $U = \mathcal{L}(X,Y)$, $V = \mathcal{L}(Y,Z)$ and $W = \mathcal{L}(X,Z)$, and let $A \in GL(U)$, $B \in GL(V)$ and $C \in GL(W)$ be transformations of U, V and W such that*

$$(Bv)(Au) = C(vu) \quad \forall\, u \in U, v \in V. \tag{5}$$

Then there exist $p \in GL(X)$, $q \in GL(Y)$, and $r \in GL(Z)$ such that A, B and C are given by rules $Au = qup^{-1}$, $Bv = rvq^{-1}$, and $Cw = rwp^{-1}$, for $u \in U$, $v \in V$ and $w \in W$, respectively.

Proof. First prove that A and B preserve type of subspaces of U and V, respectively. Clearly, $(B(N))(A(M)) = C(NM)$ for any subspaces $M \subseteq U$ and $N \subseteq V$, whence $\dim B(N)A(M) = \dim NM$, for all M and N. In particular, $\dim VA(M) = \dim VM$ for all M. Applying statement 1) of Lemma 4.20 we see that $\beta_1(A(M)) \dim Z = \beta_1(M) \dim Z$, whence $\beta_1(A(M)) = \beta_1(M)$ for any M.

Also, $B(N)A(M) = 0$ if and only if $NM = 0$, whence one easily sees that $\operatorname{ann}(A(M)) = B(\operatorname{ann}(M))$, whence

$$(\dim Y - \beta_2(A(M))) \dim Z = (\dim Y - \beta_2(M)) \dim Z,$$

whence finally $\beta_2(A(M)) = \beta_2(M)$. Thus, A preserves type of subspaces in U. Similarly one can prove that B preserves type of subspaces in V. So by Proposition 4.15 A and B have the form $Au = qup^{-1}$ and $Bv = r_1vq_1^{-1}$ for some $p \in GL(X)$, $q, q_1 \in GL(Y)$ and $r_1 \in GL(Z)$. Substituting these explicit formulae into condition (5), we see that

$$(r_1vq_1^{-1})(qup^{-1}) = C(vu) \qquad \forall\ u \in U, v \in V.$$

For any $d \in GL(Y)$ we have $(vd)(d^{-1}u) = vu$, for all $u \in U$ and $v \in V$, whence

$$(r_1vdq_1^{-1})(qd^{-1}up^{-1}) = C(vd \cdot d^{-1}u) = C(vu) = (r_1vq_1^{-1})(qup^{-1}).$$

Multiplying by r_1^{-1} on the left and by p on the right, we see that $vdq_1^{-1}qd^{-1}u = vq_1^{-1}qu$, for all $u \in U$ and $v \in V$. Applying Lemma 4.21 we see that $dq_1^{-1}qd^{-1} = q_1^{-1}q$. Thus, the element $q_1^{-1}q \in GL(Y)$ commutes with all $d \in GL(Y)$ and so must be a scalar, whence $q_1 = \lambda q$, for some $\lambda \in K^*$. So we can rewrite the formula for Bv as $Bv = r_1vq_1^{-1} = rvq^{-1}$, where $r = \lambda^{-1}r_1$. Thus, we have $Au = qup^{-1}$ and $Bv = rvq^{-1}$, for all u and v. Now

$$(rvq^{-1})(qup^{-1}) = C(vu), \quad \forall\ u \in U, v \in V,$$

whence $C(vu) = rvup^{-1}$ for all u and v. Since $\langle vu \mid u \in U, , v \in V\rangle = W$, we see that $Cw = rwp^{-1}$ for all $w \in W$. □

The following statement may be considered by the reader as an evident consequence of Proposition 4.22. Nevertheless, we give a formal proof.

Corollary 4.23 *Let $N_1 = M_{nm}$, $N_2 = M_{pn}$, $N_3 = M_{pm}$, and suppose that transformations $A_i \in GL(N_i)$, $i = 1, 2, 3$, satisfy relations $(A_2x_2)(A_1x_1) = A_3(x_2x_1)$ for all $x_1 \in N_1$ and $x_2 \in N_2$. Then there exist elements $s \in GL_m(K)$, $q \in GL_n(K)$, and $r \in GL_p(K)$ such that $A_1x_1 = qx_1s^{-1}$, $A_2x_2 = rx_2q^{-1}$, and $A_3x_3 = rx_3s^{-1}$, for all $x_i \in N_i$, $i = 1, 2, 3$.*

Proof. Let $X = K^m$, $Y = K^n$, and $Z = K^p$ be the column spaces. First we identify, in a usual way, N_1, N_2, and N_3 with $\mathcal{L}(X, Y)$, $\mathcal{L}(Y, Z)$, and $\mathcal{L}(X, Z)$, respectively.

Namely, for $h \in N_1$ let $\varphi(h) \in \mathcal{L}(X, Y)$ be the multiplication by h, i.e., $(\varphi(h))(x) = hx$, for all $x \in X$. Equivalently, for a map $g \in \mathcal{L}(X, Y)$ the corresponding element $\varphi^{-1}(g) \in N_1$

is just the matrix of g with respect to standard bases in X and Y. It is clear that $\varphi : N_1 \longrightarrow \mathcal{L}(X, Y)$ is an isomorphism of linear spaces.

In a similar way we identify N_2 with $\mathcal{L}(Y, Z)$, and N_3 with $\mathcal{L}(X, Z)$. Moreover, we identify $GL(X)$, $GL(Y)$ and $GL(Z)$ with $GL_m(K)$, $GL_n(K)$ and $GL_p(K)$, respectively. It is convenient to use the same symbol φ for all these identifications. Thus, φ is a bijection from

$$I = N_1 \sqcup N_2 \sqcup N_3 \sqcup GL_m(K) \sqcup GL_n(K) \sqcup GL_p(K)$$

to

$$J = \mathcal{L}(X, Y) \sqcup \mathcal{L}(Y, Z) \sqcup \mathcal{L}(X, Z) \sqcup GL(X) \sqcup GL(Y) \sqcup GL(Z).$$

Further, it is easy to see that φ preserves multiplication, for example, $\varphi(x_2)\varphi(x_1) = \varphi(x_2x_1)$ for any $x_1 \in N_1$ and $x_2 \in N_2$. Generally, if $x, y \in I$, and if at least one of two expressions xy and $\varphi(x)\varphi(y)$ is defined, then the other one is defined also and $\varphi(x)\varphi(y) = \varphi(xy)$. Moreover, if $x, y \in J$ and at least one of two expressions xy and $\varphi^{-1}(x)\varphi^{-1}(y)$ is defined, then the other one is defined also and $\varphi^{-1}(x)\varphi^{-1}(y) = \varphi^{-1}(xy)$.

Let B_1, B_2 and B_3 be the transformations of the spaces $\mathcal{L}(X, Y)$, $\mathcal{L}(Y, Z)$, and $\mathcal{L}(X, Z)$, corresponding to A_1, A_2 and A_3 under φ; that is, $B_i = \varphi A_i \varphi^{-1}$. Then for any $y_1 \in \mathcal{L}(X, Y)$ and $y_2 \in \mathcal{L}(Y, Z)$ we have $(B_2y_2)(B_1y_1) = B_3(y_2y_1)$. Indeed,

$$\begin{aligned}(B_2y_2)(B_1y_1) &= ((\varphi A_2\varphi^{-1})y_2)((\varphi A_1\varphi^{-1})y_1) = (\varphi(A_2(\varphi^{-1}(y_2))))(\varphi(A_1(\varphi^{-1}(y_1)))) \\ &= \varphi((A_2(\varphi^{-1}(y_2)))(A_1(\varphi^{-1}(y_1)))) = \varphi(A_3((\varphi^{-1}(y_2))(\varphi^{-1}(y_1)))) \\ &= \varphi(A_3(\varphi^{-1}(y_2y_1))) = (\varphi A_3\varphi^{-1})(y_2y_1) = B_3(y_2y_1).\end{aligned}$$

Applying Proposition 4.22, we see that there exist $s_1 \in GL(X)$, $q_1 \in GL(Y)$ and $r_1 \in GL(Z)$ such that $B_1x = q_1xs_1^{-1}$, $B_2x = r_1xq_1^{-1}$, and $B_3x = r_1xs_1^{-1}$, where $x \in \mathcal{L}(X, Y)$, $\mathcal{L}(Y, Z)$, or $\mathcal{L}(X, Z)$, respectively. Therefore for any $x \in N_1$ we have

$$\begin{aligned}A_1x &= (\varphi^{-1}B_1\varphi)(x) = \varphi^{-1}(B_1(\varphi(x))) = \varphi^{-1}(q_1\varphi(x)s_1^{-1}) \\ &= \varphi^{-1}(q_1)\varphi^{-1}(\varphi(x))\varphi^{-1}(s_1^{-1}) = qxs^{-1},\end{aligned}$$

where $s = \varphi^{-1}(s_1)$ and $q = \varphi^{-1}(q_1)$. In a similar way one can prove formulae for A_2x and A_3x (with $r = \varphi^{-1}(r_1)$). □

4.9 Proof of Proposition 4.8

We start with the following observation. Let x and y be $a \times b$ and $b \times a$ matrices, respectively. Then $\mathrm{Tr}(xy) = \mathrm{Tr}(yx)$. Moreover,

$$(x, y) \mapsto \langle x, y\rangle = \mathrm{Tr}(xy) = \mathrm{Tr}(yx)$$

is a nondegenerate bilinear pairing between M_{ab} and M_{ba}. Therefore we may identify M_{ab}^* with M_{ba}, and M_{ba}^* with M_{ab}.

Further, the group $G = GL_a(K) \times GL_b(K)$ acts on both M_{ab} and M_{ba} in a usual way, that is, $g = (g_1, g_2)$ takes $x \in M_{ab}$ and $y \in M_{ba}$ to $g_1xg_2^{-1}$ and $g_2yg_1^{-1}$, respectively. The pairing is invariant under this action. Indeed, if $x \in M_{ab}$, $y \in M_{ba}$, and $g = (g_1, g_2) \in G$, then

$$\langle gx, gy\rangle = \mathrm{Tr}((g_1xg_2^{-1})(g_2yg_1^{-1})) = \mathrm{Tr}(g_1xyg_1^{-1}) = \mathrm{Tr}(xy) = \langle x, y\rangle.$$

Therefore the transformations, induced by g on M_{ab} and M_{ba}, are contragradient each to the other.

Let $L_1 = M_{mn}$, $L_2 = M_{np}$ and $L_3 = M_{pm}$ be as in the hypothesis of the Proposition, and let $N_1 = M_{nm}$ and $N_2 = M_{pn}$. Then N_i is dual to L_i, $i = 1, 2$. Let $\varphi : N_1 \times N_2 \longrightarrow L_3$ be the usual product map, that is, $\varphi(x, y) = yx$. Its structure tensor $\widetilde{\varphi} \in N_1^* \otimes N_2^* \otimes L_3$ may be considered as an element of $L_1 \otimes L_2 \otimes L_3$. We show that $\widetilde{\varphi} = t = \langle m, n, p\rangle$.

Indeed, we have

$$t = \sum_{1\le i\le m,\ 1\le j\le n,\ 1\le k\le p} e_{ij} \otimes e_{jk} \otimes e_{ki}\,.$$

Let

$$\psi : L_1 \otimes L_2 \otimes L_3 = N_1^* \otimes N_2^* \otimes L_3 \longrightarrow \mathcal{L}_2(N_1, N_2; L_3)$$

be the canonical map, described in Subsection 4.4 (denoted by φ there). We must show that the bilinear map $\rho = \psi(t)$ coincides with φ. The bases of N_1 and N_2 are $\{e_{lq} \mid 1 \le l \le n,\ 1 \le q \le m\}$ and $\{e_{rs} \mid 1 \le r \le p,\ 1 \le s \le n\}$, respectively. It follows from the definition of ψ that the value of ρ on the pair (e_{lq}, e_{rs}) equals

$$\sum_{\substack{1\le i\le m\\ 1\le j\le n\\ 1\le k\le p}} \mathrm{Tr}(e_{ij}e_{lq})\mathrm{Tr}(e_{jk}e_{rs})e_{ki} = \sum_{\substack{1\le i\le m\\ 1\le j\le n\\ 1\le k\le p}} \delta_{jl}\delta_{iq}\delta_{kr}\delta_{js}e_{ki} = \sum_{1\le j\le n} \delta_{jl}\delta_{js}e_{rq} = \delta_{ls}e_{rq}\,.$$

On the other hand, $\varphi(e_{lq}, e_{rs}) = e_{rs}e_{lq} = \delta_{sl}e_{rq}$. Thus, $\rho(e_{lq}, e_{rs}) = \varphi(e_{lq}, e_{rs})$ for any l, q, r, and s, that is, $\varphi = \rho$. Thus, $t = \widetilde{\varphi}$.

Return to the proof of the proposition, and assume that $g \in \Gamma^0(t)$. We have $g = A_1 \otimes A_2 \otimes A_3$, for some $A_i \in GL(L_i)$, $i = 1, 2, 3$. For $i = 1, 2$ we put $B_i = A_i^\vee \in GL(L_i^*) = GL(N_i)$. Then $A_i = B_i^\vee$, $i = 1, 2$. So we have $B_1^\vee \otimes B_2^\vee \otimes A_3 \in \Gamma^0(\widetilde{\varphi})$. Now Proposition 4.14 implies that $(B_1, B_2, A_3) \in \Delta(\varphi)$. In other words, $(B_2y)(B_1x) = A_3(yx)$ for any $x \in M_{nm}$ and $y \in M_{pn}$. By Corollary 4.23, there exist $a \in GL_m(K)$, $b \in GL_n(K)$ and $c \in GL_p(K)$ such that B_1, B_2 and A_3 are defined by the rules $B_1x = bxa^{-1}$, $B_2x = cxb^{-1}$ and $A_3x = cxa^{-1}$, where $x \in N_1$, N_2, or L_3, respectively.

It follows from the discussion in the beginning of the proof that the transformation on L_1, contragredient to transformation $x \mapsto bxa^{-1}$ on N_1, may be described by the formula $x \mapsto axb^{-1}$. Similarly, A_2 acts by the rule $x \mapsto bxc^{-1}$. Therefore, g acts by

$$A(x \otimes y \otimes z) = axb^{-1} \otimes byc^{-1} \otimes cza^{-1}.$$

That is, $g = T(a, b, c)$. □

5 Automorphisms of Laderman algorithm

In this section we find automorphisms of the Laderman algorithm. The structure of the section is as follows. First we recall Laderman algorithm in its computational form, and rewrite it in the tensor form. Then we produce a certain subgroup G of $\Gamma(t)$, the isotropy group of $t = \langle 3, 3, 3\rangle$. Then we check that G preserves the algorithm. Finally, we prove that G is the full automorphism group of the algorithm. In the end of the section we give a less formal explanation on how G was found.

5.1 Laderman algorithm

Recall the description of the Laderman algorithm in computational form, according to [33]. Let

$$X = \begin{pmatrix} x_{11} & x_{12} & x_{13} \\ x_{21} & x_{22} & x_{23} \\ x_{31} & x_{32} & x_{33} \end{pmatrix} \quad \text{and} \quad Y = \begin{pmatrix} y_{11} & y_{12} & y_{13} \\ y_{21} & y_{22} & y_{23} \\ y_{31} & y_{32} & y_{33} \end{pmatrix}.$$

Consider the products

$$p_1 = (x_{11} + x_{12} + x_{13} - x_{21} - x_{22} - x_{32} - x_{33})y_{22}\,, \quad p_2 = (x_{11} - x_{21})(-y_{12} + y_{22}),$$

$$p_3 = x_{22}(-y_{11} + y_{12} + y_{21} - y_{22} - y_{23} - y_{31} + y_{33}), \quad p_4 = (-x_{11} + x_{21} + x_{22})(y_{11} - y_{12} + y_{22}),$$

$$p_5 = (x_{21} + x_{22})(-y_{11} + y_{12}), \quad p_6 = x_{11}y_{11}\,, \quad p_7 = (-x_{11} + x_{31} + x_{32})(y_{11} - y_{13} + y_{23}),$$

$$p_8 = (-x_{11} + x_{31})(y_{13} - y_{23}), \quad p_9 = (x_{31} + x_{32})(-y_{11} + y_{13}),$$

$$p_{10} = (x_{11}+x_{12}+x_{13}-x_{22}-x_{23}-x_{31}-x_{32})y_{23}\,, \quad p_{11} = x_{32}(-y_{11}+y_{13}+y_{21}-y_{22}-y_{23}-y_{31}+y_{32}),$$

$$p_{12} = (-x_{13} + x_{32} + x_{33})(y_{22} + y_{31} - y_{32}), \quad p_{13} = (x_{13} - x_{33})(y_{22} - y_{32}), \quad p_{14} = x_{13}y_{31}\,,$$

$$p_{15} = (x_{32} + x_{33})(-y_{31} + y_{32}), \quad p_{16} = (-x_{13} + x_{22} + x_{23})(y_{23} + y_{31} - y_{33}),$$

$$p_{17} = (x_{13} - x_{23})(y_{23} - y_{33}), \quad p_{18} = (x_{22} + x_{23})(-y_{31} + y_{33}), \quad p_{19} = x_{12}y_{21}\,,$$

$$p_{20} = x_{23}y_{32}\,, \quad p_{21} = x_{21}y_{13}\,, \quad p_{22} = x_{31}y_{12}\,, \quad p_{23} = x_{33}y_{33}\,.$$

Then one can check that the coefficients of the matrix

$$Z = XY = \begin{pmatrix} z_{11} & z_{12} & z_{13} \\ z_{21} & z_{22} & z_{23} \\ z_{31} & z_{32} & z_{33} \end{pmatrix}$$

can be computed according to the formulae

$$z_{11} = p_6 + p_{14} + p_{19}\,,$$

$$z_{12} = p_1 + p_4 + p_5 + p_6 + p_{12} + p_{14} + p_{15}\,,$$

$$z_{13} = p_6 + p_7 + p_9 + p_{10} + p_{14} + p_{16} + p_{18}\,,$$

$$z_{21} = p_2 + p_3 + p_4 + p_6 + p_{14} + p_{16} + p_{17}\,,$$

$$z_{22} = p_2 + p_4 + p_5 + p_6 + p_{20}\,,$$

$$z_{23} = p_{14} + p_{16} + p_{17} + p_{18} + p_{21}\,,$$

$$z_{31} = p_6 + p_7 + p_8 + p_{11} + p_{12} + p_{13} + p_{14}\,,$$

$$z_{32} = p_{12} + p_{13} + p_{14} + p_{15} + p_{22}\,,$$

$$z_{33} = p_6 + p_7 + p_8 + p_9 + p_{23}\,.$$

(In [33] there are only a few words on how this algorithm was found. The author of [33] promised to publish more detailed description of his approach, but this was never done.)

Write Laderman algorithm in tensor form. Let $M = M_{33}(K)$ $(= M_3(K)$, in traditional notation, since we consider square matrices), put $L_1 = L_2 = L_3 = M$, and put next $L = L_1 \otimes L_2 \otimes L_3$. Consider the following elements of L:

$$t_1 = (e_{11} + e_{12} + e_{13} - e_{21} - e_{22} - e_{32} - e_{33}) \otimes e_{22} \otimes e_{21}\,,$$

$$t_2 = (e_{11} - e_{21}) \otimes (-e_{12} + e_{22}) \otimes (e_{12} + e_{22})\,,$$

$$t_3 = e_{22} \otimes (-e_{11} + e_{12} + e_{21} - e_{22} - e_{23} - e_{31} + e_{33}) \otimes e_{12}\,,$$

$$t_4 = (-e_{11} + e_{21} + e_{22}) \otimes (e_{11} - e_{12} + e_{22}) \otimes (e_{21} + e_{12} + e_{22})\,,$$

$$t_5 = (e_{21} + e_{22}) \otimes (-e_{11} + e_{12}) \otimes (e_{21} + e_{22})\,,$$

$$t_6 = e_{11} \otimes e_{11} \otimes (e_{11} + e_{21} + e_{31} + e_{12} + e_{22} + e_{13} + e_{33})\,,$$

$$t_7 = (-e_{11} + e_{31} + e_{32}) \otimes (e_{11} - e_{13} + e_{23}) \otimes (e_{31} + e_{13} + e_{33})\,,$$

$$t_8 = (-e_{11} + e_{31}) \otimes (e_{13} - e_{23}) \otimes (e_{13} + e_{33})\,,$$

$$t_9 = (e_{31} + e_{32}) \otimes (-e_{11} + e_{13}) \otimes (e_{31} + e_{33})\,,$$

$$t_{10} = (e_{11} + e_{12} + e_{13} - e_{22} - e_{23} - e_{31} - e_{32}) \otimes e_{23} \otimes e_{31}\,,$$

$$t_{11} = e_{32} \otimes (-e_{11} + e_{13} + e_{21} - e_{22} - e_{23} - e_{31} + e_{32}) \otimes e_{13}\,,$$

$$t_{12} = (-e_{13} + e_{32} + e_{33}) \otimes (e_{22} + e_{31} - e_{32}) \otimes (e_{21} + e_{13} + e_{23})\,,$$

$$t_{13} = (e_{13} - e_{33}) \otimes (e_{22} - e_{32}) \otimes (e_{13} + e_{23})\,,$$

$$t_{14} = e_{13} \otimes e_{31} \otimes (e_{11} + e_{21} + e_{31} + e_{12} + e_{32} + e_{13} + e_{23})\,,$$

$$t_{15} = (e_{32} + e_{33}) \otimes (-e_{31} + e_{32}) \otimes (e_{21} + e_{23})\,,$$

$$t_{16} = (-e_{13} + e_{22} + e_{23}) \otimes (e_{23} + e_{31} - e_{33}) \otimes (e_{31} + e_{12} + e_{32})\,,$$

$$t_{17} = (e_{13} - e_{23}) \otimes (e_{23} - e_{33}) \otimes (e_{12} + e_{32})\,,$$

$$t_{18} = (e_{22} + e_{23}) \otimes (-e_{31} + e_{33}) \otimes (e_{31} + e_{32})\,,$$

$$t_{19} = e_{12} \otimes e_{21} \otimes e_{11}\,, \quad t_{20} = e_{23} \otimes e_{32} \otimes e_{22}\,,$$

$$t_{21} = e_{21} \otimes e_{13} \otimes e_{32}\,, \quad t_{22} = e_{31} \otimes e_{12} \otimes e_{23}\,,$$

$$t_{23} = e_{33} \otimes e_{33} \otimes e_{33}\,.$$

Proposition 5.1 *The set $\mathcal{L} = \{t_1\,, \ldots, t_{23}\}$ is the tensor form of the Laderman algorithm.*

Proof. A direct computation following discussion in Section 2. Alternatively, the reader can check that the sum $t_1 + \ldots + t_{23}$ coincides with $t = \langle 3, 3, 3\rangle$. □

5.2 A subgroup of $\Gamma(t)$

For $a, b, c \in GL_3(K)$ let $T(a,b,c) : L \longrightarrow L$ be the transformation, described in Subsection 4.2, defined by

$$T(a,b,c) : x \otimes y \otimes z \mapsto axb^{-1} \otimes byc^{-1} \otimes cza^{-1} \,.$$

Introduce notation for several special elements of $GL_3(K)$. Let

$$\pi_{12} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} = e_{12} + e_{21} + e_{33}$$

be the transformation, intrchanging the basis vectors e_1 and e_2, and define π_{13} and π_{23} similarly. Also put $\varepsilon_1 = \mathrm{diag}(-1,1,1)$, $\varepsilon_2 = \mathrm{diag}(1,-1,1)$, and $\varepsilon_3 = \mathrm{diag}(1,1,-1)$. Note that all matrices π_{ij} and ε_i are symmetric, and ε_i and π_{jk} commute, if $\{i,j,k\} = \{1,2,3\}$.

Further, introduce the following decomposable automorphisms Φ_i, $i = 1,2,3,4$, of L. Put

$$\Phi_1 = T(\pi_{23}, \pi_{13}, 1) : x \otimes y \otimes z \mapsto \pi_{23} x \pi_{13} \otimes \pi_{13} y \otimes z \pi_{23} \,,$$

and

$$\Phi_2 = T(\pi_{23}, 1, \pi_{23}).$$

Next, define Φ_3 and Φ_4 by

$$\Phi_3(x \otimes y \otimes z) = y^t \varepsilon_2 \otimes \varepsilon_2 x^t \otimes z^t$$

(where $x \mapsto x^t$ is the transpose map) and

$$\Phi_4(x \otimes y \otimes z) = \varepsilon_1 z \pi_{12} \otimes \pi_{12} x \pi_{12} \varepsilon_1 \otimes \varepsilon_1 \pi_{12} y \varepsilon_1 \,.$$

Proposition 5.2 *The following relations hold:*

$$\Phi_1^2 = \Phi_2^2 = \Phi_3^2 = \Phi_4^3 = 1, \quad \Phi_1\Phi_2 = \Phi_2\Phi_1 \,, \quad \Phi_3\Phi_1\Phi_3 = \Phi_1\Phi_2 \,,$$

$$\Phi_3\Phi_2\Phi_3 = \Phi_2 \,, \quad \Phi_4\Phi_1\Phi_4^{-1} = \Phi_1\Phi_2 \,, \quad \Phi_4\Phi_2\Phi_4^{-1} = \Phi_1 \,,$$

$$\Phi_3\Phi_4\Phi_3 = \Phi_4^{-1} \,.$$

Proof. The relations $\Phi_1^2 = \Phi_2^2 = 1$ and $\Phi_1\Phi_2 = \Phi_2\Phi_1$ hold because π_{13} and π_{23} are elements of order 2 in $GL_3(K)$ and $(a,b,c) \mapsto T(a,b,c)$ is a homomorphism from $GL_3(K)^{\times 3}$ to $\Gamma(t)$, as was observed in the proof of Proposition 4.5. The remaining relations may be proved by a direct calculation. Show, for example, that $\Phi_4^3 = 1$ and $\Phi_3\Phi_1\Phi_3 = \Phi_1\Phi_2$.

We have

$$\begin{aligned} x \otimes y \otimes z &\overset{\Phi_4}{\mapsto} \varepsilon_1 z \pi_{12} \otimes \pi_{12} x \pi_{12} \varepsilon_1 \otimes \varepsilon_1 \pi_{12} y \varepsilon_1 \\ &\overset{\Phi_4}{\mapsto} \varepsilon_1(\varepsilon_1 \pi_{12} y \varepsilon_1)\pi_{12} \otimes \pi_{12}(\varepsilon_1 z \pi_{12})\pi_{12}\varepsilon_1 \otimes \varepsilon_1 \pi_{12}(\pi_{12} x \pi_{12} \varepsilon_1)\varepsilon_1. \end{aligned}$$

Simplify the latter expression. We have

$$\varepsilon_1(\varepsilon_1 \pi_{12} y \varepsilon_1)\pi_{12} = \varepsilon_1^2 \pi_{12} y \varepsilon_1 \pi_{12} = \pi_{12} y \varepsilon_1 \pi_{12} \,,$$

$$\pi_{12}(\varepsilon_1 z\pi_{12})\pi_{12}\varepsilon_1 = \pi_{12}\varepsilon_1 z\pi_{12}^2\varepsilon_1 = \pi_{12}\varepsilon_1 z\varepsilon_1\,,$$

and similarly

$$\varepsilon_1\pi_{12}(\pi_{12}x\pi_{12}\varepsilon_1)\varepsilon_1 = \varepsilon_1 x\pi_{12}\,,$$

whence

$$\Phi_4^2(x\otimes y\otimes z) = \pi_{12}y\varepsilon_1\pi_{12}\otimes\pi_{12}\varepsilon_1 z\varepsilon_1\otimes\varepsilon_1 x\pi_{12}\,.$$

Consequently,

$$\Phi_4^3(x\otimes y\otimes z) = \varepsilon_1(\varepsilon_1 x\pi_{12})\pi_{12}\otimes\pi_{12}(\pi_{12}y\varepsilon_1\pi_{12})\pi_{12}\varepsilon_1\otimes\varepsilon_1\pi_{12}(\pi_{12}\varepsilon_1 z\varepsilon_1)\varepsilon_1 = x\otimes y\otimes z,$$

so the equality $\Phi_4^3 = 1$ is established.

Now we check that $\Phi_3\Phi_1\Phi_3 = \Phi_1\Phi_2$. We have

$$\begin{aligned} x\otimes y\otimes z &\overset{\Phi_3}{\mapsto} y^t\varepsilon_2\otimes\varepsilon_2 x^t\otimes z^t \overset{\Phi_1}{\mapsto} \pi_{23}(y^t\varepsilon_2)\pi_{13}\otimes\pi_{13}\varepsilon_2 x^t\otimes z^t\pi_{23} \\ &\overset{\Phi_3}{\mapsto} (\pi_{13}\varepsilon_2 x^t)^t\varepsilon_2\otimes\varepsilon_2(\pi_{23}(y^t\varepsilon_2)\pi_{13})^t\otimes(z^t\pi_{23})^t. \end{aligned}$$

Simplify the latter expression. We have

$$(\pi_{13}\varepsilon_2 x^t)^t\varepsilon_2 = (x^t)^t\varepsilon_2^t\pi_{13}^t\varepsilon_2 = x\varepsilon_2\pi_{13}\varepsilon_2 = x\pi_{13}$$

(because π_{13} and ε_2 are symmetric and commute). Similarly $\varepsilon_2(\pi_{23}(y^t\varepsilon_2)\pi_{13})^t = \varepsilon_2\pi_{13}\varepsilon_2 y\pi_{23} = \pi_{13}y\pi_{23}$, and $(z^t\pi_{23})^t = \pi_{23}z$. After all we obtain

$$(\Phi_3\Phi_1\Phi_3)(x\otimes y\otimes z) = x\pi_{13}\otimes\pi_{13}y\pi_{23}\otimes\pi_{23}z = T(1,\pi_{13},\pi_{23})(x\otimes y\otimes z),$$

whence $\Phi_3\Phi_1\Phi_3 = T(1,\pi_{13},\pi_{23})$. It remains to observe that

$$T(1,\pi_{13},\pi_{23}) = T(\pi_{23},\pi_{13},1)T(\pi_{23},1,\pi_{23}) = \Phi_1\Phi_2.$$

□

Lemma 5.3 *Let G be a group containing four elements a_1, a_2, a_3, a_4 such that*

(1) a_1, a_2, a_3, a_4 generate G,

(2) a_i satisfy relations

$$a_1^2 = a_2^2 = a_3^2 = a_4^3 = 1, \quad a_1a_2 = a_2a_1\,, \quad a_3a_1a_3 = a_1a_2\,, \tag{6}$$

$$a_3a_2a_3 = a_2\,, \quad a_4a_1a_4^{-1} = a_1a_2\,, \quad a_4a_2a_4^{-1} = a_1\,, \quad a_3a_4a_3 = a_4^{-1}\,,$$

and

(3) $a_1 \neq 1$.

Then $G \cong S_4$.

Proof. First observe that S_4 contains elements b_1, b_2, b_3, b_4, satisfying relations (6) (with a_i replaced by b_i), namely $b_1 = (12)(34)$, $b_2 = (13)(24)$, $b_3 = (13)$, and $b_4 = (123)$ (checking relations (6) is left to the reader). Also note that the system of relations (6) is equivalent to the following system of relations:

$$a_1^2 = a_2^2 = a_3^2 = a_4^3 = 1, \quad a_2a_1 = a_1a_2\,, \quad a_3a_1 = a_1a_2a_3\,, \tag{7}$$

$$a_3a_2 = a_2a_3\,, \quad a_4a_1 = a_1a_2a_4\,, \quad a_4a_2 = a_1a_4\,, \quad a_3a_4 = a_4^2a_3\,.$$

It follows that if G is any group, satisfying conditions (1) and (2) of the lemma (but not necessary (3)), then any element of G can be written in the form

$$a_1^{l_1}a_2^{l_2}a_4^{l_4}a_3^{l_3}\,, \tag{8}$$

where $0 \le l_1, l_2, l_3 \le 1$ and $0 \le l_4 \le 2$. Indeed, any element of G can be represented as a product of elements a_i, for example

$$a_2a_3^{-1}a_4^{-1}a_1 = a_2a_3a_4a_4a_1\,.$$

Next, using relations $a_3^2 = 1$, $a_3a_1 = a_1a_2a_3$, $a_3a_2 = a_2a_3$, and $a_3a_4 = a_4^2a_3$, we can transform such a product to the form $wa_3^{l_3}$, where w is a word involving only a_1, a_2, and a_4, and $l_3 \in \{0, 1\}$. For example,

$$a_2\underline{a_3a_4}a_4a_1 = a_2a_4a_4\underline{a_3a_4}a_1 = a_2a_4a_4a_4a_4\underline{a_3a_1} = a_2\underline{a_4a_4a_4a_4}a_1a_2a_3 = a_2a_4a_1a_2a_3$$

(in this chain of transformations we underline, in each step, the piece of product being transformed in this step). Similarly, using relations $a_4a_1 = a_1a_2a_4$ and $a_4a_2 = a_1a_4$, we can drag all a_4 involved in w to the right and obtain an expression of the form $va_4^{l_4}$, where v is a word involving only a_1 and a_2, and $0 \le l_4 \le 2$. Finally we can transform v to the form $a_1^{l_1}a_2^{l_2}$, where $0 \le l_1, l_2 \le 1$, using relations $a_1^2 = a_2^2 = 1$ and $a_2a_1 = a_1a_2$. After all these transformations we arrive to the word of the form (8).

Therefore, any group G that satisfies conditions (1) and (2) is of order $\le 2\cdot 2\cdot 3\cdot 2 = 24$; in particular, G is finite.

It is well known that the normal subgroups of the symmetric group S_4 are the following: the trivial group $\{e\}$, the Klein four-group

$$V = \{e,\ (12)(34),\ (13)(24),\ (14)(23)\},$$

the alternating group A_4, and the full S_4. In particular, any nontrivial normal subgroup of S_4 contains V. Observe also that $\langle b_1, b_2\rangle = V$, $b_4 \in A_4 - V$, and $b_3 \in S_4 - A_4$. Hence it is easy to see that $\langle b_1, b_2, b_4\rangle = A_4$ and $\langle b_1, b_2, b_3, b_4\rangle = S_4$.

Consider the direct product $H = G \times S_4$, and let $\pi_1 : H \longrightarrow G$ and $\pi_2 : H \longrightarrow S_4$ be the projections onto factors. Consider next the elements $c_i = (a_i, b_i) \in H$, $i = 1, 2, 3, 4$, and put $K = \langle c_1, c_2, c_3, c_4\rangle$. Then

$$\pi_1(K) = \langle \pi_1(c_1), \ldots, \pi_1(c_4)\rangle = \langle a_1, a_2, a_3, a_4\rangle = G,$$

and similarly $\pi_2(K) = S_4$. Since the elements a_i, as well as b_i, satisfy relations (6), the elements c_i satisfy these relations also, whence $|K| \le 24$. As $\pi_2|_K : K \longrightarrow S_4$ is surjective, $|K| \le 24$, and $|S_4| = 24$, we see that $\pi_2|_K$ must be an isomorphism.

Let $\rho = (\pi_2|_K)^{-1} : S_4 \longrightarrow K$ be the isomorphism, inverse to $\pi_2|_K$. Then $\sigma = \pi_1|_K \circ \rho : S_4 \longrightarrow G$ is an epimorphism. Now it is sufficient to show that the kernel of σ is trivial. It follows from the definitions that $\pi_2(c_i) = b_i$, whence $\rho(b_i) = c_i$ and $\sigma(b_i) = \pi_1(\rho(b_i)) = \pi_1(c_i) = a_i$. If $\operatorname{Ker}\sigma \ne 1$, then $\operatorname{Ker}\sigma \supseteq V \ni b_1$, because V is the only minimal normal subgroup of S_4. But $\sigma(b_1) = a_1 \ne 1$, a contradiction. Hence $\operatorname{Ker}\sigma = 1$. □

Proposition 5.4 *The group $G = \langle \Phi_1, \Phi_2, \Phi_3, \Phi_4\rangle$ is isomorphic to S_4.*

Proof. It follows from Proposition 5.2 that the elements $\Phi_i = a_i$ satisfy all conditions of Lemma 5.3. □

5.3 Invariance of $\mathcal{L}$ under G

In this subsection we prove that the Laderman algorithm $\mathcal{L}$ is invariant under the group $G = \langle \Phi_i \mid i = 1, 2, 3, 4\rangle$. To prove this, we need the following quite general statement.

Lemma 5.5 *Let G be a group acting on a set X, and $N \trianglelefteq G$ be a normal subgroup. Let $\mathcal{O}$ be an orbit of N on X. Then for any $g \in G$ the set $g\mathcal{O} = \{gm \mid m \in \mathcal{O}\}$ is also an N-orbit. In particular, if $\mathcal{O}_1$ and $\mathcal{O}_2$ are two N-orbits, $x_i \in \mathcal{O}_i$, and $g \in G$ an element such that $gx_1 = x_2$, then g bijectively maps $\mathcal{O}_1$ onto $\mathcal{O}_2$.*

This statement is well known, and we leave its proof to the reader (for a proof it suffices to note that $g(nx) = (gng^{-1})(gx)$ for any $x \in X$, $n \in N$, and $g \in G$; so, if x and y are in the same N-orbit, then gx and gy are in the same N-orbit also).

We also need to know the images of some of the tensors $t_1, \ldots, t_{23}$ under some of the transformations Φ_j.

Lemma 5.6 *The following relations hold:*

$$\begin{aligned}\Phi_1 : \quad & t_1 \mapsto t_1,\ t_2 \mapsto t_{13},\ t_3 \mapsto t_{11},\ t_4 \mapsto t_{12},\ t_5 \mapsto t_{15},\ t_6 \mapsto t_{14},\\ & t_7 \mapsto t_{16},\ t_8 \mapsto t_{17},\ t_9 \mapsto t_{18},\ t_{10} \mapsto t_{10},\ t_{19} \mapsto t_{19},\ t_{20} \mapsto t_{22},\\ & t_{21} \mapsto t_{23}\,;\end{aligned}$$

$$\begin{aligned}\Phi_2 : \quad & t_1 \mapsto t_{10},\ t_2 \mapsto t_8,\ t_3 \mapsto t_{11},\ t_4 \mapsto t_7,\ t_5 \mapsto t_9,\ t_6 \mapsto t_6,\\ & t_{19} \mapsto t_{19},\ t_{20} \mapsto t_{23}\,;\end{aligned}$$

$$\Phi_3 :\ t_6 \mapsto t_6,\ t_2 \mapsto t_5,\ t_4 \mapsto t_4,\ t_{19} \mapsto t_{19},\ t_{23} \mapsto t_{23};$$

$$\Phi_4 :\ t_1 \mapsto t_3 \mapsto t_6,\ t_2 \mapsto t_2,\ t_4 \mapsto t_4,\ t_5 \mapsto t_5,\ t_{19} \mapsto t_{19},\ t_{23} \mapsto t_{23}\,.$$

Proof. A direct computation. Prove, for example, that $\Phi_1(t_3) = t_{11}$, $\Phi_4(t_1) = t_3$, and $\Phi_3(t_2) = t_5$.

We have $t_3 = e_{22} \otimes (-e_{11} + e_{12} + e_{21} - e_{22} - e_{23} - e_{31} + e_{33}) \otimes e_{12}$. The transformation Φ_1 acts by $\Phi_1(x \otimes y \otimes z) = \pi_{23}x\pi_{13} \otimes \pi_{13}y \otimes z\pi_{23}$. Hence

$$\Phi_1(t_3) = \pi_{23}e_{22}\pi_{13} \otimes \pi_{13}(-e_{11} + e_{12} + e_{21} - e_{22} - e_{23} - e_{31} + e_{33}) \otimes e_{12}\pi_{23}\,.$$

Simplify multiplicands in the latter product. We have $e_{12}\pi_{23} = e_{12}(e_{11}+e_{23}+e_{32}) = e_{12}e_{23} = e_{13}$. Generally, for any $i = 1, 2, 3$ we have $e_{i1}\pi_{23} = e_{i1}$, $e_{i2}\pi_{23} = e_{i3}$, and $e_{i3}\pi_{23} = e_{i2}$. That is, the multiplication of e_{ij} by π_{23} on the right affects only the index j, by the rule $1 \mapsto 1$, $2 \leftrightarrow 3$. Similarly we can find any product of the form $\pi e_{ij}\pi'$, where $\pi, \pi' \in \{\pi_{12}, \pi_{13}, \pi_{23}\}$. In particular, $\pi_{23}e_{22}\pi_{13} = e_{32}$.

Next, $\pi_{13}(-e_{11}+e_{12}+e_{21}-e_{22}-e_{23}-e_{31}+e_{33}) = -e_{31}+e_{32}+e_{21}-e_{22}-e_{23}-e_{11}+e_{13}$. Thus we obtain

$$\Phi_1(t_3) = e_{32} \otimes (-e_{31} + e_{32} + e_{21} - e_{22} - e_{23} - e_{11} + e_{13}) \otimes e_{13}\,,$$

which coincide with t_{11}.

Similarly we have $t_1 = (e_{11}+e_{12}+e_{13}-e_{21}-e_{22}-e_{32}-e_{33})\otimes e_{22}\otimes e_{21}$ and $\Phi_4(x\otimes y\otimes z) = \varepsilon_1 z\pi_{12}\otimes \pi_{12}x\pi_{12}\varepsilon_1\otimes \varepsilon_1\pi_{12}y\varepsilon_1$, whence

$$\Phi_4(t_1) = \varepsilon_1 e_{21}\pi_{12}\otimes \pi_{12}(e_{11}+e_{12}+e_{13}-e_{21}-e_{22}-e_{32}-e_{33})\pi_{12}\varepsilon_1\otimes \varepsilon_1\pi_{12}e_{22}\varepsilon_1\,.$$

Simplify. For any i and j we have $\varepsilon_1 e_{1j} = -e_{1j}$ and $\varepsilon_1 e_{ij} = e_{ij}$ if $i = 2$ or 3; similarly $e_{i1}\varepsilon_1 = -e_{i1}$ and $e_{ij}\varepsilon_1 = e_{ij}$ if $j = 2, 3$. Hence

$$\varepsilon_1 e_{21}\pi_{12} = e_{21}\pi_{12} = e_{22}\,, \quad \varepsilon_1\pi_{12}e_{22}\varepsilon_1 = \varepsilon_1\pi_{12}e_{22} = \varepsilon_1 e_{12} = -e_{12}\,,$$

and

$$\begin{aligned}\pi_{12}(e_{11}+e_{12}+e_{13}-e_{21}-e_{22}-e_{32}-e_{33})\pi_{12}\varepsilon_1 &= (e_{22}+e_{21}+e_{23}-e_{12}-e_{11}-e_{31}-e_{33})\varepsilon_1\\ &= e_{22}-e_{21}+e_{23}-e_{12}+e_{11}+e_{31}-e_{33}\,.\end{aligned}$$

Thus we obtain

$$\Phi_4(t_1) = e_{22}\otimes(e_{22}-e_{21}+e_{23}-e_{12}+e_{11}+e_{31}-e_{33})\otimes(-e_{12}),$$

which is equal to t_3.

Finally, $t_2 = (e_{11}-e_{21})\otimes(-e_{12}+e_{22})\otimes(e_{12}+e_{22})$ and $\Phi_3(x\otimes y\otimes z) = y^t\varepsilon_2\otimes\varepsilon_2 x^t\otimes z^t$, whence

$$\begin{aligned}\Phi_3(t_2) &= (-e_{12}+e_{22})^t\varepsilon_2\otimes\varepsilon_2(e_{11}-e_{21})^t\otimes(e_{12}+e_{22})^t = (-e_{21}+e_{22})\varepsilon_2\otimes\varepsilon_2(e_{11}-e_{12})\otimes(e_{21}+e_{22})\\ &= (-e_{21}-e_{22})\otimes(e_{11}-e_{12})\otimes(e_{21}+e_{22}) = (e_{21}+e_{22})\otimes(-e_{11}+e_{12})\otimes(e_{21}+e_{22})\\ &= t_5\,.\end{aligned}$$

□

Proposition 5.7 *The set $\mathcal{L}$ is invariant under the group $G = \langle\Phi_1, \Phi_2, \Phi_3, \Phi_4\rangle$.*

Proof. We will consider the action of G on the set of all decomposable tensors in $L = L_1\otimes L_2\otimes L_3$.

First show that $\mathcal{L}$ is invariant under Φ_1, and break it into the orbits under the cyclic group $\langle\Phi_1\rangle_2$. By Lemma 5.6 we have $\Phi_1(t_2) = t_{13}$. As $\Phi_1^2 = 1$, we have also $\Phi_1(t_{13}) = \Phi_1(\Phi_1(t_2)) = t_2$, so $\{t_2, t_{13}\}$ is a $\langle\Phi_1\rangle_2$-orbit. We abbreviate $\{t_2, t_{13}\}$ to $\{2, 13\}$. Similarly it follows from Lemma 5.6 that

$$\omega_1 = \{1\}, \quad \omega_2 = \{2, 13\}, \quad \omega_3 = \{3, 11\}, \quad \omega_4 = \{4, 12\},$$

$$\omega_5 = \{5, 15\}, \quad \omega_6 = \{6, 14\}, \quad \omega_7 = \{7, 16\}, \quad \omega_8 = \{8, 17\},$$

$$\omega_9 = \{9, 18\}, \quad \omega_{10} = \{10\}, \quad \omega_{11} = \{19\}, \quad \omega_{12} = \{20, 22\},$$

$$\text{and} \quad \omega_{13} = \{21, 23\},$$

are $\langle\Phi_1\rangle_2$-orbits. In particular, $\mathcal{L}$ is $\langle\Phi_1\rangle_2$-invariant.

Next consider the subgroup $H_1 = \langle\Phi_1, \Phi_2\rangle$. As Φ_1 and Φ_2 commute, $\langle\Phi_1\rangle_2$ is normal in H_1. As $\Phi_2(t_2) = t_8$ and $\Phi_2^2 = 1$, we have $\Phi_2(t_8) = t_2$. Now it follows from Lemma 5.5, applied to $\langle\Phi_1\rangle_2 \trianglelefteq H_1$, that Φ_2 bijectively maps $\omega_2 = \{2, 13\}$ and $\omega_8 = \{8, 17\}$ each onto the other. Therefore

$$\omega_2 \cup \omega_8 = \{2, 13, 8, 17\} = \{2, 8, 13, 17\}$$

is an H_1-orbit. Similarly we see that the following sets are H_1-orbits:

$$\Omega_1 = \{1, 10\} = \omega_1 \cup \omega_{10}\,, \quad \Omega_2 = \{2, 8, 13, 17\} = \omega_2 \cup \omega_8\,, \quad \Omega_3 = \{3, 11\} = \omega_3\,,$$

$$\Omega_4 = \{4, 7, 12, 16\} = \omega_4 \cup \omega_7\,, \quad \Omega_5 = \{5, 9, 15, 18\} = \omega_5 \cup \omega_9\,, \quad \Omega_6 = \{6, 14\} = \omega_6\,,$$

$$\Omega_7 = \{19\} = \omega_{11}\,, \quad \Omega_8 = \{20, 21, 22, 23\} = \omega_{12} \cup \omega_{13}\,.$$

Further we consider subgroup $H_2 = \langle\Phi_1, \Phi_2, \Phi_4\rangle$. It follows from relations $\Phi_4\Phi_1\Phi_4^{-1} = \Phi_1\Phi_2$ and $\Phi_4\Phi_2\Phi_4^{-1} = \Phi_1$ that Φ_4 normalizes H_1, so H_1 is normal in H_2. Similarly, the relations $\Phi_3^2 = 1$, $\Phi_3\Phi_1\Phi_3 = \Phi_1\Phi_2$, $\Phi_3\Phi_2\Phi_3 = \Phi_2$, and $\Phi_3\Phi_4\Phi_3 = \Phi_4^{-1}$ imply that Φ_3 normalizes H_2, so $H_2 \trianglelefteq G$.

(One can observe (though this is not necessary) that under the isomorphism between G and S_4, described in the proofs of Lemma 5.3 and Proposition 5.4, the subgroups H_1 and H_2 correspond to normal subgroups V and A_4 of S_4.)

By Lemma 5.6 Φ_4 permutes cyclically t_1, t_3, and t_6. So by Lemma 5.5 Φ_4 cyclically permutes the H_1-orbits $\Omega_1 = \{1, 10\}$, $\Omega_3 = \{3, 11\}$, and $\Omega_6 = \{6, 14\}$. Therefore the set $\Sigma_1 = \Omega_1 \cup \Omega_3 \cup \Omega_6 = \{1, 3, 6, 10, 11, 14\}$ is an H_2-orbit. Next, as each of the tensors t_i, where $i = 2, 4, 5, 19, 23$, is Φ_4-invariant, we see that each of the H_1-orbits Ω_2, Ω_4, Ω_5, Ω_7, and Ω_8 is Φ_4-invariant, and therefore is an H_2-orbit.

As Φ_3 interchanges t_2 and t_5 and normalizes H_2, it interchanges the H_2-orbits Ω_2 and Ω_5. Therefore $\Sigma_2 = \Omega_2 \cup \Omega_5$ is a G-orbit. Next, as Φ_3 fixes elements $t_6 \in \Sigma_1$, $t_4 \in \Omega_4$, $t_{19} \in \Omega_7$, and $t_{23} \in \Omega_8$, we see that Φ_3 leaves invariant their H_2-orbits Σ_1, Ω_4, Ω_7, and Ω_8. Thus we obtain that the sets $\Sigma_1 = \{1, 3, 6, 10, 11, 14\}$, $\Sigma_2 = \Omega_2 \cup \Omega_5 = \{2, 5, 8, 9, 13, 15, 17, 18\}$, $\Omega_4 = \{4, 7, 12, 16\}$, $\Omega_7 = \{19\}$, and $\Omega_8 = \{20, 21, 22, 23\}$ are G-orbits. So their union $\mathcal{L} = \Sigma_1 \cup \Sigma_2 \cup \Omega_4 \cup \Omega_7 \cup \Omega_8$ is invariant under G. □

5.4 The full group $\mathrm{Aut}(\mathcal{L})$

According to Proposition 5.7, the group $G = \langle\Phi_i \mid i = 1, 2, 3, 4\rangle$ is a subgroup of $\mathrm{Aut}(\mathcal{L})$. In this subsection we prove that G is the *full* automorphism group of $\mathcal{L}$.

Let $\mathrm{Aut}(\mathcal{L})_0 \le \mathrm{Aut}(\mathcal{L})$ be the subgroup of all elements that correspond to the identity permutation of $\{L_1, L_2, L_3\}$. Also put $Q_1 = \langle\Phi_3, \Phi_4\rangle$.

Lemma 5.8 $\mathrm{Aut}(\mathcal{L}) = \mathrm{Aut}(\mathcal{L})_0 Q_1$.

Proof. Let $\pi : \Gamma(t) \longrightarrow S_3$ be the homomorphism taking each $g \in \Gamma(t)$ to the corresponding permutation of $\{L_1, L_2, L_3\}$. Then $\pi(\Phi_4) = (123)$ and $\pi(\Phi_3) = (12)(3)$, whence $\pi(Q_1) = \langle(123), (12)(3)\rangle = S_3$. Therefore for each element $g \in \mathrm{Aut}(\mathcal{L})$ there exists an element $g' \in Q_1$ such that $\pi(g) = \pi(g')$. Put $g'' = g(g')^{-1}$, then $g = g''g'$. Also $\pi(g'') = \pi(g)\pi(g')^{-1} = e$, and therefore $g'' \in \mathrm{Aut}(\mathcal{L})_0$. So $g \in \mathrm{Aut}(\mathcal{L})_0 Q_1$. As g was an arbitrary element of $\mathrm{Aut}(\mathcal{L})$, we obtain that $\mathrm{Aut}(\mathcal{L}) = \mathrm{Aut}(\mathcal{L})_0 Q_1$. □

It follows from Proposition 4.8 that the elements of $\mathrm{Aut}(\mathcal{L})_0$ are precisely the elements of $\mathrm{Aut}(\mathcal{L})$ of the form $g = T(a, b, c)$, for some $a, b, c \in GL_3(K)$.

Introduce a notion which will play important role in the rest of the paper.

Tensor projections. Let $U \otimes V$ be the product of two spaces. For any two subspaces $X, Y \subseteq U$ we have $X \otimes V \cap Y \otimes V = (X \cap Y) \otimes V$. It follows that for any subspace $L \subseteq U \otimes V$ there exists the least (i.e., the unique minimal) subspace $X \subseteq U$ such that $L \subseteq X \otimes V$. We call X the *tensor projection* of L to U, and denote this by $X = \mathrm{tpr}_U L$.

The tensor projection $\mathrm{tpr}_V L$ to the second factor is defined similarly. Also, for an element $x \in U \otimes V$ we write $\mathrm{tpr}_U x$ for $\mathrm{tpr}_U \langle x \rangle$.

Generally, if $\widetilde{U} = U_1 \otimes \ldots \otimes U_m$ is the product of several spaces, and $\overline{U} = U_{i_1} \otimes \ldots \otimes U_{i_l}$, where $1 \le i_1 < \ldots < i_l \le m$, is a "subproduct", then we can define $\mathrm{tpr}_{\overline{U}} L$, the tensor projection to $\overline{U}$, for any subspace $L \subseteq \widetilde{U}$.

It is more or less clear that operation of taking tensor projections has transitivity property; for example,

$$\mathrm{tpr}_{U_2}(\mathrm{tpr}_{U_1 \otimes U_2} L) = \mathrm{tpr}_{U_2} L$$

for any $L \subseteq U_1 \otimes U_2 \otimes U_3$.

Let $U \otimes V$ be the product of two spaces, and $X \subseteq U \otimes V$ be a set of nonzero elements of $U \otimes V$. Define

$$\mathrm{tpr}_U X = \{\mathrm{tpr}_U x \mid x \in X\}. \tag{9}$$

This is a set of nonzero subspaces of U. It may happen that $\mathrm{tpr}_U x = \mathrm{tpr}_U y$ for two distinct $x, y \in X$, $x \neq y$. So we shall consider $\mathrm{tpr}_U X$ as a *multiset*, i.e., a set with multiplicities (at least in the case if X is finite). Note that we can define $\mathrm{tpr}_U X$ by formula (9) for a multiset X also.

The operation of taking tensor projections has certain invariance properties. The following lemma is evident, but its accurate proof (which is left to the reader) may be tedious.

Lemma 5.9 *Let $\widetilde{U} = U_1 \otimes \ldots \otimes U_m$ be a tensor product of several spaces, $X \subseteq \widetilde{U}$ be a finite (multi)subset of nonzero tensors, and let $\varphi \in S(U_1, \ldots, U_m)$ be a decomposable automorphism of $\widetilde{U}$ such that $\varphi(X) = X$. Suppose that φ takes factor U_i to U_j, and let $\psi : U_i \longrightarrow U_j$ be the corresponding isomorphism (ψ is defined up to constant). Then ψ takes (multi)set $\mathrm{tpr}_{U_i} X$ to $\mathrm{tpr}_{U_j} X$.*

Return to considering group $\mathrm{Aut}(\mathcal{L})$. We need the following lemma.

Lemma 5.10 *Let $V = \langle e_1, e_2, e_3 \rangle$ be a three-dimensional space, and let $\pi_{23} \in GL(V)$ acts by $\pi_{23} : e_1 \mapsto e_1$, $e_2 \leftrightarrow e_3$. Let $\varphi \in GL(V)$ be a transformation preserving the multiset of lines*

$$\mathcal{X} = \{1 \cdot \langle e_1 \rangle, 4 \cdot \langle e_2 \rangle, 4 \cdot \langle e_3 \rangle, 2 \cdot \langle e_1 - e_2 \rangle, 2 \cdot \langle e_1 - e_3 \rangle\}.$$

Then either $\varphi = \lambda \cdot \mathrm{id}_V$ or $\varphi = \lambda \pi_{23}$, where $\lambda \in K^*$.

Proof. It is clear that φ preserves each of the three sets of lines $\{\langle e_1 \rangle\}$, $\{\langle e_2 \rangle, \langle e_3 \rangle\}$, and $\{\langle e_1 - e_2 \rangle, \langle e_1 - e_3 \rangle\}$. So φ either leaves each of the lines $\langle e_i \rangle$ invariant, or preserves $\langle e_1 \rangle$ and interchanges $\langle e_2 \rangle$ and $\langle e_3 \rangle$.

In the first case we have $\varphi(e_i) = a_i e_i$, where $a_i \in K^*$. Then $\varphi(e_1 - e_2) = a_1 e_1 - a_2 e_2$. The latter vector must be proportional to $e_1 - e_2$ or to $e_1 - e_3$, so it is proportional to $e_1 - e_2$ and $a_1 = a_2$. Similarly $a_1 = a_3$, and therefore $\varphi = a_1 \cdot \mathrm{id}_V$.

In the second case φ acts as $e_1 \mapsto a_1 e_1$, $e_2 \mapsto a_2 e_3$, $e_3 \mapsto a_3 e_2$. The line $\langle e_1 - e_2 \rangle$ goes to $\langle a_1 e_1 - a_2 e_3 \rangle$, whence $a_2 = a_1$. Similarly $a_3 = a_1$, and therefore $\varphi = a_1 \pi_{23}$. □

Lemma 5.11 *Consider the following set of one-dimensional subspaces in the space $M = M_{33}(K)$:*

$$\begin{aligned}\mathcal{C} = \{ \quad & \langle e_{11} - e_{21}\rangle, \langle e_{21} + e_{22}\rangle, \langle -e_{11} + e_{31}\rangle, \langle e_{31} + e_{32}\rangle, \langle e_{13} - e_{33}\rangle, \langle e_{32} + e_{33}\rangle, \\ & \langle e_{13} - e_{23}\rangle, \langle e_{22} + e_{23}\rangle, \langle e_{12}\rangle, \langle e_{23}\rangle, \langle e_{21}\rangle, \langle e_{31}\rangle, \langle e_{33}\rangle\}.\end{aligned}$$

Let $a, b \in GL_3(K)$ be elements such that the transformation $\varphi : x \mapsto axb$ preserves $\mathcal{C}$. Then

$$a \in \{1, \pi_{23}\} \quad \textit{and} \quad b \in \{1, \pi_{13}\}$$

up to scalar factors.

Proof. Let V and V' be spaces of 3-columns and 3-rows, respectively. We can identify $M = M_3(K)$ with $V \otimes V'$ by the isomorphism $\alpha : V \otimes V' \longrightarrow M_3(K)$ defined by $\alpha(v \otimes v') = vv'$ (cf. Subsection 4.1).

Note that a matrix $x \in M$ is of rank 1 if and only if the corresponding tensor $\alpha^{-1}(x) \in V \otimes V'$ is decomposable, $\alpha^{-1}(x) = v \otimes v'$. The set $\mathcal{C}' = \alpha^{-1}(\mathcal{C})$, corresponding to $\mathcal{C}$ under α, consists of 13 lines in $V \otimes V'$ spanned by decomposable tensors, namely

$$\begin{aligned}\mathcal{C}' = \alpha^{-1}(\mathcal{C}) = \{ \quad & \langle (e_1 - e_2) \otimes e^1\rangle, \langle e_2 \otimes (e^1 + e^2)\rangle, \langle (e_1 - e_3) \otimes e^1\rangle, \\ & \langle e_3 \otimes (e^1 + e^2)\rangle, \langle (e_1 - e_3) \otimes e^3\rangle, \langle e_3 \otimes (e^2 + e^3)\rangle, \langle (e_1 - e_2) \otimes e^3\rangle, \\ & \langle e_2 \otimes (e^2 + e^3)\rangle, \langle e_1 \otimes e^2\rangle, \langle e_2 \otimes e^3\rangle, \langle e_2 \otimes e^1\rangle, \langle e_3 \otimes e^1\rangle, \langle e_3 \otimes e^3\rangle\}.\end{aligned}$$

Let $\varphi' : V \otimes V' \longrightarrow V \otimes V'$ be the automorphism corresponding to φ under α, that is, $\varphi' = \alpha^{-1}\varphi\alpha$. It is easy to see that φ' is decomposable, namely $\varphi' = \varphi_1 \otimes \varphi_2$, where $\varphi_1 : V \longrightarrow V$ and $\varphi_2 : V' \longrightarrow V'$ are defined by $\varphi_1(x) = ax$ and $\varphi_2(y) = yb$. Indeed, for any $v \in V$ and $v' \in V'$ we have

$$\begin{aligned}\varphi'(v \otimes v') &= (\alpha^{-1}\varphi\alpha)(v \otimes v') = \alpha^{-1}(\varphi(\alpha(v \otimes v'))) = \alpha^{-1}(\varphi(vv')) = \alpha^{-1}(avv'b) \\ &= \alpha^{-1}((av)(v'b)) = av \otimes v'b = \varphi_1(v) \otimes \varphi_2(v') = (\varphi_1 \otimes \varphi_2)(v \otimes v').\end{aligned}$$

Since $\mathcal{C}$ is invariant under φ, we see that $\mathcal{C}'$ must be invariant under φ'. Therefore the tensor projections $\mathrm{tpr}_V\mathcal{C}' = \mathcal{C}'_1$ and $\mathrm{tpr}_{V'}\mathcal{C}' = \mathcal{C}'_2$ must be invariant (as multisets) under φ_1 and φ_2, respectively.

We can immediately see that

$$\mathcal{C}'_1 = \{1 \cdot \langle e_1\rangle, 4 \cdot \langle e_2\rangle, 4 \cdot \langle e_3\rangle, 2 \cdot \langle e_1 - e_2\rangle, 2 \cdot \langle e_1 - e_3\rangle\}$$

and

$$\mathcal{C}'_2 = \{4 \cdot \langle e^1\rangle, 1 \cdot \langle e^2\rangle, 4 \cdot \langle e^3\rangle, 2 \cdot \langle e^1 + e^2\rangle, 2 \cdot \langle e^2 + e^3\rangle\}.$$

It follows from Lemma 5.10 that $a = 1$ or $a = \pi_{23}$, up to a scalar. Similarly one can prove that $b = 1$ or $b = \pi_{13}$ up to a scalar. □

Proposition 5.12 *The equality* $\mathrm{Aut}(\mathcal{L})_0 = \langle \Phi_1, \Phi_2\rangle$ *holds.*

Proof. The inclusion $\mathrm{Aut}(\mathcal{L})_0 \supseteq \langle\Phi_1, \Phi_2\rangle$ is obvious, because both Φ_1 and Φ_2 are of the form $T(a, b, c)$. We need to prove the inverse inclusion.

Let $u = u_1 \otimes u_2 \otimes u_3$ be a decomposable tensor of $L_1 \otimes L_2 \otimes L_3$. The triple $(\mathrm{rk}(u_1), \mathrm{rk}(u_2), \mathrm{rk}(u_3))$ will be called the *type* of u. The tensors of type $(1, 1, 1)$ in $\mathcal{L}$ are t_i with $i = 2$, 5, 8, 9, 13,15, 17, 18, 19, 20, 21, 22, 23, of type $(2, 1, 1)$ — t_i with $i = 1, 10$, $(1, 2, 1)$ — with $i = 3, 11$, $(1, 1, 2)$ — $i = 6, 14$, and $(2, 2, 2)$ — $i = 4$, 7, 12, 16 (and there are no tensors of other types, say $(2, 2, 3)$, in $\mathcal{L}$).

By $\mathcal{B}$ we denote the set of all t_i of type $(1, 1, 1)$.

Observe that for any $x \in GL_3(K)$ and $y \in M_3(K)$ we have $\mathrm{rk}(xy) = \mathrm{rk}(yx) = \mathrm{rk}(y)$. Hence for arbitrary decomposable tensor $u = u_1 \otimes u_2 \otimes u_3 \in L$ and arbitrary transformation of the form $g = T(a, b, c)$ the types of tensors u and $g(u)$ coincide. It follows that any element $g \in \mathrm{Aut}(\mathcal{L})_0$ preserves $\mathcal{B}$.

Further, let $g = T(a, b, c)$ be any element of $\mathrm{Aut}(\mathcal{L})_0$. As g preserves $\mathcal{B}$, the set of tensor projections $\mathcal{C} = \mathrm{tpr}_{L_1}\mathcal{B}$ must be invariant under transformation $\varphi : x \mapsto axb^{-1}$. It is easy to see that

$$\begin{aligned}\mathcal{C} = \{ \quad & \langle e_{11} - e_{21}\rangle, \langle e_{21} + e_{22}\rangle, \langle -e_{11} + e_{31}\rangle, \langle e_{31} + e_{32}\rangle, \langle e_{13} - e_{33}\rangle, \langle e_{32} + e_{33}\rangle, \\ & \langle e_{13} - e_{23}\rangle, \langle e_{22} + e_{23}\rangle, \langle e_{12}\rangle, \langle e_{23}\rangle, \langle e_{21}\rangle, \langle e_{31}\rangle, \langle e_{33}\rangle\}.\end{aligned}$$

By Lemma 5.11, g has the form $g = T(\pi_{23}^{\varepsilon}, \pi_{13}^{\eta}, c)$, for some $\varepsilon, \eta \in \{0, 1\}$. Remembering that $\Phi_1 = T(\pi_{23}, \pi_{13}, 1)$ and $\Phi_2 = T(\pi_{23}, 1, \pi_{23})$, we see that there exist (uniquely defined) $\gamma, \delta \in \{0, 1\}$ and g' of the form $g' = T(1, 1, c')$ such that $g = \Phi_1^{\varepsilon}\Phi_2^{\eta}g'$. So it is sufficient to show that any element g' of the form $g' = T(1, 1, c')$, leaving $\mathcal{B}$ invariant, coincide with the identity map.

Obviously, g' acts on L_1 trivially (up to a scalar). Note also that the tensor projections of all elements of $\mathcal{B}$ to L_1 are pairwise distinct. It follows that g' fixes each element of $\mathcal{B}$. So the map $x \mapsto xc^{-1}$ preserves any subspace of the form $\mathrm{tpr}_{L_2}v$, where $v \in \mathcal{B}$. Hence easily follows (by an argument similar to the proof of Lemma 5.11) that c is a scalar, whence $g' = 1$. □

Thus, the statement of Theorem 1.1, concerning the Laderman algorithm, is established.

5.5 Some details of calculations

In the arguments of Subsections 5.2–5.4 we used the transformations Φ_1, Φ_2, Φ_3, Φ_4 "in ready form", but the reader may ask (and the author should explain) how these transformations were *found*. (Though, it is not difficult to have an idea of this from arguments of Subsection 5.4).

The key idea is to decompose each of the spaces $L_i = M_{3,3}$ $(i = 1, 2, 3)$ as $L_i = U_i \otimes V_i$, where U_i (resp., V_i) are three copies of the space of 3-columns (resp., 3-rows). Then $L = L_1 \otimes L_2 \otimes L_3$ decomposes as

$$L = U_1 \otimes V_1 \otimes U_2 \otimes V_2 \otimes U_3 \otimes V_3\,. \tag{10}$$

It follows from Theorem 4.12 that any element of $\Gamma(t)$ is a decomposable automorphism of L with respect to decomposition (10). Next, a decomposable tensor $u = u_1 \otimes u_2 \otimes u_3 \in L$ is decomposable with respect to (10) if and only if it is of type $(1, 1, 1)$. It was noted above that $\mathrm{Aut}(\mathcal{L})$ must preserve the set $\mathcal{B}$ of all elements of $\mathcal{L}$ of type $(1, 1, 1)$.

We can consider $\mathcal{B}$ as a set of 13 tensors decomposable with respect to (10). It is convenient to write $\mathcal{B}$ as a table (see Table 1).

Figure 1: Table 1

N	U_1	V_1	U_2	V_2	U_3	V_3
2	$1-2$	1	$-1+2$	2	$1+2$	2
5	2	$1+2$	1	$-1+2$	2	$1+2$
8	$-1+3$	1	$1-2$	3	$1+3$	3
9	3	$1+2$	1	$-1+3$	3	$1+3$
13	$1-3$	3	$2-3$	2	$1+2$	3
15	3	$2+3$	3	$-1+2$	2	$1+3$
17	$1-2$	3	$2-3$	3	$1+3$	2
18	2	$2+3$	3	$-1+3$	3	$1+2$
19	1	2	2	1	1	1
20	2	3	3	2	2	2
21	2	1	1	3	3	2
22	3	1	1	2	2	3
23	3	3	3	3	3	3

For example, the 3-rd row of the table reads as follows:

$$t_8 = (-e_1 + e_3) \otimes e^1 \otimes (e_1 - e_2) \otimes e^3 \otimes (e_1 + e_3) \otimes e^3 = (-e_{11} + e_{31}) \otimes (e_{13} - e_{23}) \otimes (e_{13} + e_{33}).$$

Assume that $g \in \mathrm{Aut}(\mathcal{L})$ preserves each of the factors L_1, L_2, and L_3. Then g has the form $g = T(a, b, c)$, in particular g preserves all factors U_i, V_i of decomposition (10). Since g preserves $\mathcal{B}$, it follows that the transformation $x \mapsto ax$ preserves the multiset

$$\mathrm{tpr}_{U_1}\mathcal{B} = \{1 \cdot \langle e_1 \rangle, 4 \cdot \langle e_2 \rangle, 4 \cdot \langle e_3 \rangle, 2 \cdot \langle e_1 - e_2 \rangle, 2 \cdot \langle e_1 - e_3 \rangle\},$$

whence $a = 1$ or $a = \pi_{23}$, up to a scalar. Similarly one can show that $b = \pi_{13}^{\eta}$ and $c = \pi_{23}^{\theta}$, for some $\eta, \theta \in Z_2 = \{0, 1\}$. Therefore

$$g = T(\pi_{23}^{\varepsilon}, \pi_{13}^{\eta}, \pi_{23}^{\theta})$$

for some $\varepsilon, \eta, \theta \in Z_2$. It is easy to check that any element of the latter form with $\varepsilon + \theta + \eta = 0$ preserves $\mathcal{B}$, while the element with $(\varepsilon, \eta, \theta) = (0, 0, 1)$ (and therefore any element with $\varepsilon + \theta + \eta = 1$) does not.

Then the author has checked that elements with $\varepsilon + \theta + \eta = 0$ preserve the set $\mathcal{L} \setminus \mathcal{B}$ (i.e., the set of all elements of $\mathcal{L}$ whose type is different from $(1, 1, 1)$) also, and so preserve the whole $\mathcal{L}$. Thus, the group $\mathrm{Aut}(\mathcal{L}) \cap \Gamma^0(t)$ turns out to be completely described.

Next we should consider elements of $\mathrm{Aut}(\mathcal{L})$ corresponding to nontrivial permutation of the factors L_1, L_2, and L_3.

The observation that $\mathcal{L}$ contains 13 and 4 elements of types $(1, 1, 1)$ and $(2, 2, 2)$, respectively, and 2 elements of each of the types $(2, 1, 1)$, $(1, 2, 1)$, and $(1, 1, 2)$, suggests that the group of permutations of factors induced by $\mathrm{Aut}(\mathcal{L})$ is either Z_3 or S_3.

Indeed, using Lemma 5.9 and the table above, it is not hard to find candidates for automorphisms corresponding to nontrivial permutations of L_1, L_2, L_3. A candidate for an automorphism corresponding to (12)(3) can be found from the table very easily. In fact, this candidate is nothing else but Φ_3. As to an automorphism corresponding to (123), to find it is a more complicated task.

Finally note that the checking that $\mathcal{L}$ is invariant under all Φ_i was made by the author directly, without using Lemma 5.5 and relations of Proposition 5.2. (These relations were found later, in order to streamline the argument in the present text.)

6 Automorphisms of the Hopcroft algorithm

6.1 Hopcroft algorithm

Recall the description of the Hopcroft algorithm (in computational form), according to [24]. Let

$$X = \begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \\ x_{31} & x_{32} \end{pmatrix}, \quad \text{and} \quad Y = \begin{pmatrix} y_{11} & y_{12} & y_{13} \\ y_{21} & y_{22} & y_{23} \end{pmatrix}.$$

Then the coefficients z_{ij} of the matrix

$$Z = XY = \begin{pmatrix} z_{11} & z_{12} & z_{13} \\ z_{21} & z_{22} & z_{23} \\ z_{31} & z_{32} & z_{33} \end{pmatrix}$$

can be computed by formulae

$$z_{11} = p_1 + p_2\,, \quad z_{22} = p_3 + p_4\,, \quad z_{33} = p_5 + p_6\,,$$

$$z_{12} = -p_2 - p_3 + p_7 - p_8\,, \quad z_{21} = -p_1 - p_4 + p_8 - p_9\,,$$

$$z_{13} = -p_1 - p_5 - p_{13} + p_{15}\,, \quad z_{31} = -p_2 - p_6 + p_{13} - p_{14}\,,$$

$$z_{23} = -p_3 - p_6 + p_{11} - p_{12}\,, \quad z_{32} = -p_4 - p_5 + p_{10} - p_{11}\,,$$

where

$$p_1 = (x_{11} - x_{12})y_{11}\,, \quad p_2 = x_{12}(y_{11} + y_{21}), \quad p_3 = x_{21}y_{12}\,,$$

$$p_4 = x_{22}y_{22}\,, \quad p_5 = x_{31}(y_{13} + y_{23}), \quad p_6 = (-x_{31} + x_{32})y_{23}\,,$$

$$p_7 = (x_{11} + x_{21})(y_{11} + y_{12} + y_{21} + y_{22}),$$

$$p_8 = (x_{11} - x_{12} + x_{21})(y_{11} + y_{21} + y_{22}),$$

$$p_9 = (x_{11} - x_{12} + x_{21} - x_{22})(y_{21} + y_{22}),$$

$$p_{10} = (x_{22} + x_{32})(y_{12} + y_{13} + y_{22} + y_{23}),$$

$$p_{11} = (x_{22} - x_{31} + x_{32})(y_{12} + y_{13} + y_{23}),$$

$$p_{12} = (-x_{21} + x_{22} - x_{31} + x_{32})(y_{12} + y_{13}),$$

$$p_{13} = (x_{12} + x_{31})(y_{11} - y_{23}), \quad p_{14} = (-x_{12} - x_{32})(y_{21} + y_{23}),$$

$$p_{15} = (x_{11} + x_{31})(y_{11} + y_{13}).$$

Further, present Hopcroft algorithm in tensor form. Consider the following decomposable tensors in the space $M_{32} \otimes M_{23} \otimes M_{33}$:

$$t_1 = (e_{11} - e_{12}) \otimes e_{11} \otimes (e_{11} - e_{31} - e_{12}),$$

$$t_2 = e_{12} \otimes (e_{11} + e_{21}) \otimes (e_{11} - e_{21} - e_{13}),$$
$$t_3 = e_{21} \otimes e_{12} \otimes (-e_{21} + e_{22} - e_{32}),$$
$$t_4 = e_{22} \otimes e_{22} \otimes (-e_{12} + e_{22} - e_{23}),$$
$$t_5 = e_{31} \otimes (e_{13} + e_{23}) \otimes (e_{33} - e_{31} - e_{23}),$$
$$t_6 = (-e_{31} + e_{32}) \otimes e_{23} \otimes (e_{33} - e_{13} - e_{32}),$$
$$t_7 = (e_{11} + e_{21}) \otimes (e_{11} + e_{12} + e_{21} + e_{22}) \otimes e_{21}\,,$$
$$t_8 = (e_{11} - e_{12} + e_{21}) \otimes (e_{11} + e_{21} + e_{22}) \otimes (e_{12} - e_{21}),$$
$$t_9 = (e_{11} - e_{12} + e_{21} - e_{22}) \otimes (e_{21} + e_{22}) \otimes (-e_{12}),$$
$$t_{10} = (e_{22} + e_{32}) \otimes (e_{12} + e_{13} + e_{22} + e_{23}) \otimes e_{23}\,,$$
$$t_{11} = (e_{22} - e_{31} + e_{32}) \otimes (e_{12} + e_{13} + e_{23}) \otimes (-e_{23} + e_{32}),$$
$$t_{12} = (-e_{21} + e_{22} - e_{31} + e_{32}) \otimes (e_{12} + e_{13}) \otimes (-e_{32}),$$
$$t_{13} = (e_{12} + e_{31}) \otimes (e_{11} - e_{23}) \otimes (e_{13} - e_{31}),$$
$$t_{14} = (e_{12} + e_{32}) \otimes (e_{21} + e_{23}) \otimes e_{13}\,,$$
$$t_{15} = (e_{11} + e_{31}) \otimes (e_{11} + e_{13}) \otimes e_{31}\,.$$

Proposition 6.1 *The set $\mathcal{H} = \{t_1\,, \ldots, t_{15}\}$ is the tensor form of the Hopcroft algorithm.*

Proof. A direct computation, left to the reader. □

6.2 The group $\mathrm{Aut}(\mathcal{H})$

In this subsection we find the automorphism group of the Hopcroft algorithm. Our arguments are similar to those for Laderman's algorithm, cf. Subsections 5.2–5.4. So we provide only the results of computations,usually, leaving the details to the reader.

Let $L_1 = M_{32}$, $L_2 = M_{23}$, $L_3 = M_{33}$, and $L = L_1 \otimes L_2 \otimes L_3$. We can consider transformations of L of the form $T(a, b, c)$, where $a, c \in GL_3(K)$ and $b \in GL_2(K)$.

Put $d = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \in GL_2(K)$, then $d^3 = 1$ and $d^{-1} = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$. Also put

$$\pi_{123} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Let e_{ij} be a matrix unit in one of the spaces M_{32}, M_{23}, or M_{33}. Observe that the multiplication of the matrix e_{ij} by π_{123} on the left, resp. by π_{123}^{-1} on the right, shifts the subscript i (resp., j) by 1: $\pi_{123} e_{ij} = e_{i+1,j}$ (if the product $\pi_{123} e_{ij}$ makes sense, that is, if $e_{ij} \in M_{32}$ or

M_{33}), and similarly $e_{ij}\pi_{123}^{-1} = e_{i,j+1}$, if $e_{ij} \in M_{23}$ or M_{33}. Here subscripts $i+1$ ($j+1$) are taken modulo 3, so that $3+1=1$.

Consider transformations

$$\Phi_1 = T(\pi_{123}, d, \pi_{123}) : x \otimes y \otimes z \mapsto \pi_{123} x \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix} \otimes \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} y \pi_{123}^{-1} \otimes \pi_{123} z \pi_{123}^{-1} \,,$$

$$\Phi_2 = T(\pi_{13}, \pi_{12}, \pi_{13}) : x \otimes y \otimes z \mapsto \pi_{13} x \pi_{12} \otimes \pi_{12} y \pi_{13} \otimes \pi_{13} z \pi_{13} \,,$$

and

$$\Phi_3 : x \otimes y \otimes z \mapsto y^t \pi_{12} \varepsilon_1 \otimes \varepsilon_1 \pi_{12} x^t \otimes z^t$$

(here notation π_{12}, π_{13}, and ε_1 have the same meaning as in Subsection 5.2).

Lemma 6.2 *The transformations Φ_1, Φ_2, and Φ_3 satisfy the following relations:*

$$\Phi_1^3 = \Phi_2^2 = \Phi_3^2 = 1, \quad \Phi_2 \Phi_1 \Phi_2 = \Phi_1^{-1},$$

$$\Phi_3 \Phi_1 = \Phi_1 \Phi_3 \,, \quad \Phi_3 \Phi_2 = \Phi_2 \Phi_3 \,.$$

Proof. Recall that the map by the rule $(a,b,c) \mapsto T(a,b,c)$ is a group homomorphism (from $GL_3(K) \times GL_2(K) \times GL_3(K)$ to $GL(L)$). So the relations $\Phi_1^3 = \Phi_2^2 = 1$ follow from $\pi_{123}^3 = \pi_{13}^2 = 1$ and $d^3 = \pi_{12}^2 = 1$. Similarly, the relation $\Phi_2\Phi_1\Phi_2 = \Phi_1^{-1}$ follows from $\pi_{13}\pi_{123}\pi_{13} = \pi_{123}^{-1}$ and $\pi_{12} d \pi_{12} = d^{-1}$. The remaining three relations can be proved by direct computations (cf. the proof of Proposition 5.2). □

Lemma 6.3 *Let G be a group generated by three elements a_1, a_2, a_3. Suppose that a_i satisfy relations*

$$a_1^3 = a_2^2 = a_3^2 = 1, \quad a_2 a_1 a_2 = a_1^{-1} \,, \quad a_3 a_1 = a_1 a_3 \,, \quad a_3 a_2 = a_2 a_3 \,. \tag{11}$$

Suppose also that $a_1 \neq 1$ and $a_3 \neq 1$. Then $G \cong S_3 \times Z_2$.

Proof. The argument is similar to that in the proof of Lemma 5.3. Note first that system (11) is equivalent to

$$a_1^3 = a_2^2 = a_3^2 = 1, \quad a_2 a_1 = a_1^2 a_2 \,, \quad a_3 a_1 = a_1 a_3 \,, \quad a_3 a_2 = a_2 a_3 \,. \tag{12}$$

Next, consider the group $S_3 \times Z_2$. The elements of Z_2 will be denoted by 0 and 1. In $S_3 \times Z_2$ consider the elements $b_1 = ((123), 0)$, $b_2 = ((12), 0)$, and $b_3 = (e, 1)$. Clearly, they satisfy relations (11) and (12).

Further, observe that if X is any group generated by three elements c_i satisfying relations (12) (with a_i replaced by c_i), then any element of X can be written as $c_1^{l_1} c_2^{l_2} c_3^{l_3}$, where $0 \le l_1 \le 2$, $0 \le l_2, l_3 \le 1$. Hence $|X| \le 12 = |S_3 \times Z_2|$.

Finally, it is easy to see that any minimal normal subgroup of $S_3 \times Z_2$ is either $\langle b_1 \rangle_3$ or $\langle b_3 \rangle_2$.

Using the facts observed it is not hard to give a proof similar to that of Lemma 5.3. The details are left to the reader. □

The following statement is an obvious corollary of Lemmas 6.2 and 6.3.

Corollary 6.4 *The group $G = \langle \Phi_1, \Phi_2, \Phi_3 \rangle$ is isomorphic to $S_3 \times Z_2$.*

Lemma 6.5 *The following relations for action of transformations Φ_i on tensors t_j hold:*

$$\begin{aligned}
\Phi_1 : \quad & t_1 \mapsto t_4 \mapsto t_5\,, \quad t_2 \mapsto t_3 \mapsto t_6\,, \quad t_7 \mapsto t_{12} \mapsto t_{14}\,, \\
& t_9 \mapsto t_{10} \mapsto t_{15}\,, \quad t_8 \mapsto t_{11} \mapsto t_{13}\,; \\
\Phi_2 : \quad & t_1 \mapsto t_6\,, \quad t_{14} \mapsto t_{15}\,, \quad t_8 \mapsto t_{11}\,; \\
\Phi_3 : \quad & t_1 \mapsto t_2\,, \quad t_7 \mapsto t_9\,, \quad t_8 \mapsto t_8\,.
\end{aligned}$$

Proof. A direct computation. □

Proposition 6.6 *Consider the action of the group $G = \langle \Phi_1, \Phi_2, \Phi_3 \rangle$ on the set of nonzero decomposable tensors in L. Then the sets*

$$\Omega_1 = \{t_1, \dots, t_6\} = \{1, 2, 3, 4, 5, 6\},$$

$$\Omega_2 = \{7, 9, 10, 12, 14, 15\},$$

and

$$\Omega_3 = \{8, 11, 13\}$$

are G-orbits. In particular, the set

$$\mathcal{H} = \Omega_1 \cup \Omega_2 \cup \Omega_3 = \{t_1, \dots, t_{15}\}$$

is invariant under G.

Proof. The argument is similar to the proof of Proposition 5.7. First of all, it follows from Lemma 6.5 and the relation $\Phi_1^3 = 1$ that the sets

$$\omega_1 = \{t_1, t_4, t_5\} = \{1, 4, 5\}, \quad \omega_2 = \{2, 3, 6\}, \quad \omega_3 = \{7, 12, 14\},$$

$$\omega_4 = \{8, 11, 13\}, \quad \text{and} \quad \omega_5 = \{9, 10, 15\}$$

are orbits of the group $\langle \Phi_1 \rangle_3$. Next, as Φ_2 normalizes $\langle \Phi_1 \rangle_3$, it follows from Lemma 5.5 and the relation

$$\Phi_2 : t_1 \mapsto t_6\,, \quad t_{14} \mapsto t_{15}\,, \quad t_8 \mapsto t_{11}\,,$$

that Φ_2 interchanges ω_1 and ω_2, ω_3 and ω_5, and preserves ω_4. So the sets $\Omega_1 = \omega_1 \cup \omega_2$, $\Omega_2 = \omega_3 \cup \omega_5$, and $\Omega_3 = \omega_4$, are orbits under the group $\langle \Phi_1, \Phi_2 \rangle$. Finally, as Φ_3 normalizes (even centralizes) $\langle \Phi_1, \Phi_2 \rangle$, it follows from the action of Φ_3 on t_1, t_7, and t_8, that each of the $\langle \Phi_1, \Phi_2 \rangle$-orbits Ω_1, Ω_2, and Ω_3 is invariant under Φ_3. So Ω_i is an orbit under G. □

Corollary 6.7 *$G = \langle \Phi_1, \Phi_2, \Phi_3 \rangle$ is a subgroup of* $\mathrm{Aut}(\mathcal{H})$.

In the rest of this section we prove that, in fact, $\mathrm{Aut}(\mathcal{H}) = G$.

Let $\mathrm{Aut}(\mathcal{H})_0 \le \mathrm{Aut}(\mathcal{H})$ be the subgroup of all elements preserving each of the factors L_1, L_2, and L_3. The following lemma and its proof are similar to Lemma 5.8.

Lemma 6.8 *We have* $\mathrm{Aut}(\mathcal{H}) = \mathrm{Aut}(\mathcal{H})_0 \langle \Phi_3 \rangle_2$.

Proof. Let $\pi : \Gamma(t) \longrightarrow S_3$ be the homomorphism that assigns to each element $g \in \Gamma(t)$ the corresponding permutation of the factors L_1, L_2, and L_3. As $\dim L_1 = \dim L_2 = 6$ and $\dim L_3 = 9$, we have $\pi(\Gamma(t)) \subseteq \{e, (12)(3)\}$ (and, actually, $\pi(\Gamma(t)) = \{e, (12)(3)\}$ by Theorem 4.12). On the other hand, it is clear that $\pi(\Phi_3) = (12)(3)$. The rest of the proof is similar to that of Lemma 5.8. □

Let V and V' be spaces of 3-columns and 3-rows, respectively, (e_1, e_2, e_3) and (e^1, e^2, e^3) be the usual bases of V and V', and let $GL_3(K)$ acts on V and V' in the usual way. Let $\sigma \in S_3$ be a permutation. By $\widetilde{\sigma}$ we denote the element of $GL_3(K)$ permuting basis vectors (e_i) according to σ.

Lemma 6.9 *Let $\varphi \in GL_3(K)$ be an element such that the sets of three lines*

$$\mathcal{X} = \{\langle e_1 + e_2\rangle, \langle e_1 + e_3\rangle, \langle e_2 + e_3\rangle\}$$

and

$$\mathcal{Y} = \{\langle e^1\rangle, \langle e^2\rangle, \langle e^3\rangle\}$$

in V and V' are invariant under φ. Then $\varphi = \lambda\widetilde{\sigma}$ for some $\sigma \in S_3$ and $\lambda \in K^*$.

Proof. Note that for any $\sigma \in S_3$ the transformation $\widetilde{\sigma}$ preserves both $\mathcal{X}$ and $\mathcal{Y}$. Moreover, the permutation by which $\widetilde{\sigma}$ acts on $\mathcal{Y}$ coincides with σ. Now let φ be as in the hypothesis of the lemma, and σ be the permutation by which φ acts on $\mathcal{Y}$. Then the transformation $\varphi' = \widetilde{\sigma}^{-1}\varphi$ leaves each of the lines $\langle e^i\rangle$ invariant. Therefore $\varphi' = \operatorname{diag}(\lambda_1, \lambda_2, \lambda_3)$ for some $\lambda_i \in K^*$. Also, φ' preserves $\mathcal{X}$. So the line $\varphi'(\langle e_1 + e_2\rangle) = \langle \lambda_1 e_1 + \lambda_2 e_2\rangle$ must be in $\mathcal{X}$, and therefore it coincides with $\langle e_1 + e_2\rangle$, whence $\lambda_1 = \lambda_2$. Similarly $\lambda_1 = \lambda_3$, whence $\varphi' = \operatorname{diag}(\lambda_1, \lambda_1, \lambda_1) = \lambda_1 E$. So $\varphi = \widetilde{\sigma}\varphi' = \lambda_1\widetilde{\sigma}$. □

Proposition 6.10 *The equality* $\operatorname{Aut}(\mathcal{H})_0 = \langle \Phi_1, \Phi_2\rangle$ *holds.*

Proof. The argument is mainly similar to the proof of Proposition 5.12. Any element of $\operatorname{Aut}(\mathcal{H})_0$ is of the form $T(a, b, c)$, for some $(a, b, c) \in GL_3(K) \times GL_2(K) \times GL_3(K)$.

For any $m, n \in \mathbb{N}$ (not necessary $m = n$) and any $x \in GL_m(K)$, $y \in GL_n(K)$, $z \in M_{mn}$ we have $\operatorname{rk}(xz) = \operatorname{rk}(zy) = \operatorname{rk}(z)$. So for any decomposable tensor $u = u_1 \otimes u_2 \otimes u_3 \in M_{mn} \otimes M_{np} \otimes M_{pm}$ and any element $g = T(a, b, c)$, where $a \in GL_m(K)$, $b \in GL_n(K)$, $c \in GL_p(K)$, the tensors u and $g(u)$ are of the same type. Therefore $\operatorname{Aut}(\mathcal{H})_0$ preserves the subset of all tensors of type $(1, 1, 1)$ in $\mathcal{H}$. It is easy to see that this subset is

$$\Omega_2 = \{t_i \mid i = 7, 9, 10, 12, 14, 15\}.$$

Thus, it is sufficient to prove the following statement:

> $(*)$ *If a transformation $g = T(a, b, c)$, where $a, c \in GL_3(K)$ and $b \in GL_2(K)$, leaves the set Ω_2 invariant, then $g \in \langle \Phi_1, \Phi_2\rangle$.*

Let D and F (resp., D' and F') be two copies of the space of 3-columns (resp., 3-rows), and let E and E' be spaces of 2-columns and 2-rows, respectively. Consider tensor product

$$N = D \otimes E' \otimes E \otimes F' \otimes F \otimes D'.$$

We can identify N with $L = M_{32} \otimes M_{23} \otimes M_{33}$ by the isomorphism $\tau : N \longrightarrow L$ defined by

$$\tau(d \otimes e' \otimes e \otimes f' \otimes f \otimes d') = de' \otimes ef' \otimes fd'$$

(cf. Subsection 4.2).

Let $\mathcal{B}$ and g' be the subset and the transformation of N, corresponding to Ω_2 and g, respectively, with respect to the isomorphism τ. That is, $\mathcal{B} = \tau^{-1}(\Omega_2)$ and $g' = \tau^{-1}g\tau$. Then $g'(\mathcal{B}) = (\tau^{-1}g\tau)(\tau^{-1}(\Omega_2)) = \tau^{-1}(g(\Omega_2)) = \tau^{-1}(\Omega_2) = \mathcal{B}$, that is, g' preserves $\mathcal{B}$.

It is easy to write $\mathcal{B}$ and g' explicitly. Namely,

$$\begin{aligned}\mathcal{B} = \{ \quad & (e_1 + e_2) \otimes e^1 \otimes (e_1 + e_2) \otimes (e^1 + e^2) \otimes e_2 \otimes e^1, \\ & (e_1 + e_2) \otimes (-e^1 + e^2) \otimes e_2 \otimes (e^1 + e^2) \otimes e_1 \otimes e^2, \\ & (e_2 + e_3) \otimes e^2 \otimes (e_1 + e_2) \otimes (e^2 + e^3) \otimes e_2 \otimes e^3, \\ & (e_2 + e_3) \otimes (e^1 - e^2) \otimes e_1 \otimes (e^2 + e^3) \otimes e_3 \otimes e^2, \\ & (e_1 + e_3) \otimes e^2 \otimes e_2 \otimes (e^1 + e^3) \otimes e_1 \otimes e^3, \\ & (e_1 + e_3) \otimes e^1 \otimes e_1 \otimes (e^1 + e^3) \otimes e_3 \otimes e^1 \}.\end{aligned}$$

Also it is easy to see that g' acts according to the formula

$$g'(d \otimes e' \otimes e \otimes f' \otimes f \otimes d') = ad \otimes e'b^{-1} \otimes be \otimes f'c^{-1} \otimes cf \otimes d'a^{-1}. \tag{13}$$

Indeed, we have

$$g(\tau(d \otimes e' \otimes e \otimes f' \otimes f \otimes d')) = g(de' \otimes ef' \otimes fd')$$
$$= T(a, b, c)(de' \otimes ef' \otimes fd') = ade'b^{-1} \otimes bef'c^{-1} \otimes cfd'a^{-1}.$$

But the latter expression coincides with

$$\tau(ad \otimes e'b^{-1} \otimes be \otimes f'c^{-1} \otimes cf \otimes d'a^{-1}).$$

Therefore,

$$g'(d \otimes e' \otimes e \otimes f' \otimes f \otimes d') = (\tau^{-1}g\tau)(d \otimes e' \otimes e \otimes f' \otimes f \otimes d')$$
$$= \tau^{-1}(ade'b^{-1} \otimes bef'c^{-1} \otimes cfd'a^{-1}) = ad \otimes e'b^{-1} \otimes be \otimes f'c^{-1} \otimes cf \otimes d'a^{-1},$$

which proves formula (13).

Equality $g'(\mathcal{B}) = \mathcal{B}$, together with formula (13), imply that the tensor projection $\mathrm{tpr}_D\mathcal{B}$ is invariant under the transformation $d \mapsto ad$ $(d \in D)$. It is immediately seen that

$$\mathrm{tpr}_D\mathcal{B} = \{\langle e_1 + e_2\rangle, \langle e_1 + e_3\rangle, \langle e_2 + e_3\rangle\}.$$

Therefore the transformation $d \mapsto ad$ preserves the latter set. Similarly,

$$\mathrm{tpr}_{D'}\mathcal{B} = \{\langle e^1\rangle, \langle e^2\rangle, \langle e^3\rangle\}$$

must be invariant under transformation $d' \mapsto d'a^{-1}$. So the element $a \in GL_3(K)$ satisfies hypothesys of Lemma 6.9, whence $a = \lambda\widetilde{\sigma}$ for some $\lambda \in K^*$ and a permutation $\sigma \in S_3$. Thus, $g = T(\lambda\widetilde{\sigma}, b, c) = T(\widetilde{\sigma}, b, c)$.

Remembering that $\Phi_1 = T(\pi_{123}, \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \pi_{123})$ and $\Phi_2 = T(\pi_{13}, \pi_{12}, \pi_{13})$, and taking into account that (123) and (13)(2) generate S_3, we see that there exists an element $g_1 \in \langle \Phi_1, \Phi_2 \rangle$ of the form $g_1 = T(\widetilde{\sigma}, b_1, c_1)$. Therefore the element $g_2 = g_1^{-1} g$ is of the form $T(1, b_2, c_2)$. Moreover, it is clear that g_2 preserves Ω_2. So it is sufficient to show that if an element g_2 of the form $T(1, b_2, c_2)$ preserves Ω_2, then $g_2 \in \langle \Phi_1, \Phi_2 \rangle$. We shall prove even more, namely that $g_2 = 1$.

Let $g_2' = \tau^{-1} g_2 \tau$ be the transformation of N, corresponding to g_2. Clearly, g_2' preserves $\mathcal{B}$. Further, formula (13) immediately implies that for any element $v \in N$ the tensor projections of v and $g_2'(v)$ to $D \otimes D'$ coincide:

$$\mathrm{tpr}_{D\otimes D'} g_2'(v) = \mathrm{tpr}_{D\otimes D'} v, \quad \forall\, v \in N.$$

But the tensor projections of all elements of $\mathcal{B}$ to $D \otimes D'$ are pairwise distinct, whence $g_2'(v) = v$. That is, g_2' fixes each element of $\mathcal{B}$. It follows that the transformation $f \mapsto c_2 f$ preserves tensor projection to F of each element of $\mathcal{B}$, so preserves each of three lines $\langle e_1 \rangle$, $\langle e_2 \rangle$, and $\langle e_3 \rangle$. Similarly, the transformation $f' \mapsto f' c_2^{-1}$ preserves F'-projection of each element of $\mathcal{B}$, that is, preserves each of the three lines $\langle e^1 + e^2 \rangle$, $\langle e^1 + e^3 \rangle$, and $\langle e^2 + e^3 \rangle$. Hence easily follows that c_2 is a scalar.

Finally, the transformation $e \mapsto b_2 e$ preserves tensor projection to E of each element of $\mathcal{B}$, and therefore preserves each of the lines $\langle e_1 \rangle$, $\langle e_2 \rangle$, and $\langle e_1 + e_2 \rangle$. Hence b_2 is a scalar also.

As both b_2 and c_2 are scalars, we obtain that $g_2 = T(1, b_2, c_2) = 1$ $(= \mathrm{id}_L)$. □

We summarize the results of the present section in the following proposition.

Proposition 6.11 *The group* $\mathrm{Aut}(\mathcal{H})$ *coincides with* $G = \langle \Phi_1, \Phi_2, \Phi_3 \rangle$. *The latter group is isomorphic to* $S_3 \times Z_2$.

The latter proposition proves the part of Theorem 1.1 concerning the Hopcroft algorithm.

References

[1] A.V.Aho, J.E.Hopcroft, J.D.Ullman. *The Design and Analisys of Computer Algorithms.* Addison-Wesley, 1974.

[2] Valery B.Alekseyev, On the complexity of some algorithms of matrix multiplication, J. Algorithms 6 (1985), 71–85.

[3] V.B.Alekseev, A.V.Smirnov, On the exact and approximate bilinear complexities of multiplication of 4×2 and 2×2 matrices. Sovremennye problemy matematiki, 2013, issue 17, 135–152 (in Russian); also see `http://mi.mathnet.ru/eng/book1483`. English translation: Proc. of the Steklov Institute of Mathematics (Supplementary Issues), 2013, 282, suppl.1, S123–S139; Springer.

[4] V.B.Alekseev, On bilinear complexity of multiplication of 5×2 matrix by 2×2 matrix. Uchenye Zapiski Kazanskogo Universiteta (= Proceeding of the Kazan University), 156:3, 2014, 19–29. (`http://mi.mathnet.ru/eng/uzku1262`) (in Russian).

[5] M.Artin, *Algebra*, Prentice Hall, 1991.

[6] D.Bini, M.Capovani, F.Romani, G.Lotti, $O(n^{2,7799})$ complexity for $n \times n$ approximate matrix multiplication, Inform. Process. Letters 8:5 (1979), 234–235.

[7] M.Bläser, Lower bounds for the multiplicative complexity of matrix multiplication, Computational Complexity 8 (1999), 203–226.

[8] M.Bläser, On the complexity of the multiplication of matrices of small formats, J.Complexity 19 (2003), 43–60.

[9] M.Bläser. *Fast Matrix Multiplication* / Theory of Computing Library. Graduate Surveys 5 (2013), pp. 1–60. (www.theoryofcomputing.org).

[10] R.P.Brent, Algorithms for matrix multiplication. Technical report 70-157, Stanford University, Computer Science Department, 1970. Available at `http://maths-people.anu.edu.au/~brent/pub/pub002.html`

[11] A.E.Brouwer, A.M.Cohen, A.Neumaier, *Distance Regular Graphs*, Springer, 1989.

[12] P.Bürgisser, M.Clausen and M.A.Shokrollahi, *Algebraic Complexity Theory*, Springer, 1997.

[13] V.P.Burichenko, On symmetries of the Strassen algorithm / arXiv: 1408.6273, 2014.

[14] N.T.Courtois, G.V.Bard, D.Hulme, A new general-purpose method to multiply 3×3 matrices using only 23 multiplications / arXiv 1108.2830v3.

[15] J.H.Conway, N.J.A.Sloane, *Sphere Packings, Lattices and Groups*, Springer, 1988.

[16] C.W.Curtis, I.Reiner, *Representation Theory of Finite Groups and Associative Algebras*, Interscience Publishers, 1962.

[17] J.Dieudonné, *La geometrie des groupes classiques*, 3me éd, Springer, 1971.

[18] C.E.Drevet, M.N.Islam, E.Schost, Optimization techniques for small matrix multiplication, Theor. Comput. Sci. 412:22 (2011), 2219–2236.

[19] D.S.Dummit, R.M.Foote, *Abstract Algebra*, Wiley, 2004.

[20] H.F. de Groote, On varieties of optimal algorithms for the computation of bilinear mappings. I. The isotropy group of a bilinear mapping, Theor. Comput. Sci. 7 (1978), 1–24.

[21] H.F. de Groote, On varieties of optimal algorithms for the computation of bilinear mappings. II. Optimal algorithms for 2×2 matrix multiplication, Theor. Comput. Sci. 7 (1978), 127–148.

[22] H.F. de Groote. *Lectures on the Complexity of Bilinear Problems.* Lect. Notes Comp. Sci. 245. Springer, 1987.

[23] J.E.Hopcroft, L.R.Kerr, On minimizing the number of multiplications necessary for matrix multiplication, SIAM J. Appl. Math. 20:1 (1971), 30–36.

[24] J.Hopcroft, J.Musinski, Duality applied to the complexity of matrix multiplication and other bilinear forms, SIAM J. Comput. 2:3 (1973), 159–173.

[25] T.W.Hungerford, *Algebra*, Prentice Hall, 1991.

[26] G.James, M.Liebeck, *Representations and Characters of Groups*, 2nd ed, CUP, 2001.

[27] R.W.Johnson, A.M.MacLoughlin, Noncommutative bilinear algorithms for 3 × 3 matrix multiplication, SIAM J. Comput. 15:2 (1986), 595–603.

[28] M.I.Kargapolov, Ju.I.Merzljakov, *Fundamentals of the Theory of Groups*, Springer, 1979. (in Russian: M.I.Kargapolov, Ju.I.Merzljakov, *Osnovy Teorii Grupp*, (3rd ed.), Nauka, 1982.)

[29] D.E.Knuth. *The Art of Computer Programming,* 3rd ed, vol.2: Seminumerical algorithms. Addison-Wesley, 1997.

[30] T.G.Kolda, B.W.Bader, Tensor decompositions and applications, SIAM Review 51:3 (2009), 455–500.

[31] A.I.Kostrikin, *Introduction to Algebra*, Nauka, 1977. (in Russian)

[32] A.I.Kostrikin, Yu.I.Manin, *Linear Algebra and Geometry.* 2nd ed., Gordon and Breach, 1997.

[33] J.Laderman, A noncommutative algorithm for multiplying 3 × 3 matrices using 23 multiplications, Bull. Amer. Math. Soc. 82 (1976), 126–128.

[34] J.M.Landsberg, Geometry and the complexity of matrix multiplication, Bull. AMS 45:2 (2008), 247–284.

[35] S.Lang, *Algebra*, 3rd ed., Springer, 2002.

[36] O.M.Makarov, An algorithm for multiplying 3 × 3 matrices, Zh. Vychisl. Mat. Mat. Fiz., 26:2 (1986), 293–294; `http:// mi.mathnet.ru/eng/zvmmf4056` (in Russian). English translation: USSR Computational Mathematics and Mathematical Physics, 26:1 (1986), 179–180.

[37] Jinsoo Oh, Jin Kim, Byung-Ro Moon, On the inequivalence of bilinear algorithms for 3 × 3 matrix multiplication, Inform. Process. Letters 113:17 (2013), 640–645.

[38] V.Ya.Pan. Strassen algorithm is not optimal. Trilinear technique of aggregating, uniting and cancelling for constructing fast algorithms for matrix multiplication. Proc. 19th Annual conference on Foundations of Computer Science, Ann Arbor, 1979; pp. 166–176.

[39] V.Pan, *How to Multiply Matrices Faster*, Lect. Notes Comp.Sci. 179, Springer 1984.

[40] A.V.Smirnov, The bilinear complexity and practical algorithms for matrix multiplication, Zh. Vychisl. Mat. Mat. Fiz. 53:12 (2013), 1970–1984 (in Russian); `http://mi.mathnet.ru/eng/zvmmf9955`. English translation: Computational Mathematics and Mathematical Physics 53:12 (2013), 1781–1795.

[41] A.J.Stothers, *On the Complexity of Matrix Multiplication*, Ph.D. dissertation, University of Edinburgh, 2010.

[42] V.Strassen, Gaussian elimination is not optimal, Numer. Math. 13:4 (1969), 354–356.

[43] M.Suzuki, *Group Theory I*, Springer 1981.

[44] Virginia Vassilevska Williams, Multiplying matrices faster than Coppersmith-Winograd / STOC'12: Proceedings of the 44th annual ACM Symposium on Theory of Computing; pp.887–898.

[45] Virginia Vassilevska Williams, Breaking the Coppersmith-Winograd barrier, manuscript (available in the Internet).

[46] S.Winograd, On multiplication of 2×2 matrices, Linear Algebra Appl. 4(1971), 381–388.

[47] S.Winograd, A new algorithm for inner product, IEEE Trans. on Computers, vol.C-17, issue 7, 693–694.

[48] T.Yokonuma, *Tensor Spaces and Exterior Algebra*, AMS, 1992.

[49] D.V.Zhdanovich, The matrix capacity of a tensor, Fundamentalnaya i prikladnaya matematika 17:2 (2011/2012), 107–166 (in Russian); see also `http://mi.mathnet.ru/eng/fpm1404`. English translation: J. of Mathematical Sciences (New York) 186:4 (2012), 599–643.